

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
16 August 2001 (16.08.2001)

PCT

(10) International Publication Number
WO 01/60013 A1

(51) International Patent Classification⁷: H04L 29/06,
H04Q 7/38

[CH/CH]; Avenue de la Gare 13, CH-1800 Vevey (CH).
LAUPER, Eric [CH/CH]; Schützenweg 12, CH-3014 Bern
(CH).

(21) International Application Number: PCT/CH00/00438

(74) Agent: SAAM, Christophe; Patents & Technology Surveys SA, Faubourg du Lac 2, P.O. Box 1448, CH-2001 Neuchâtel (CH).

(22) International Filing Date: 16 August 2000 (16.08.2000)

(71) Applicant (for all designated States except US): SWISS-COM MOBILE AG [CH/CH]; Schwarztorstrasse 61, CH-3050 Bern (CH).

(81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(25) Filing Language: English

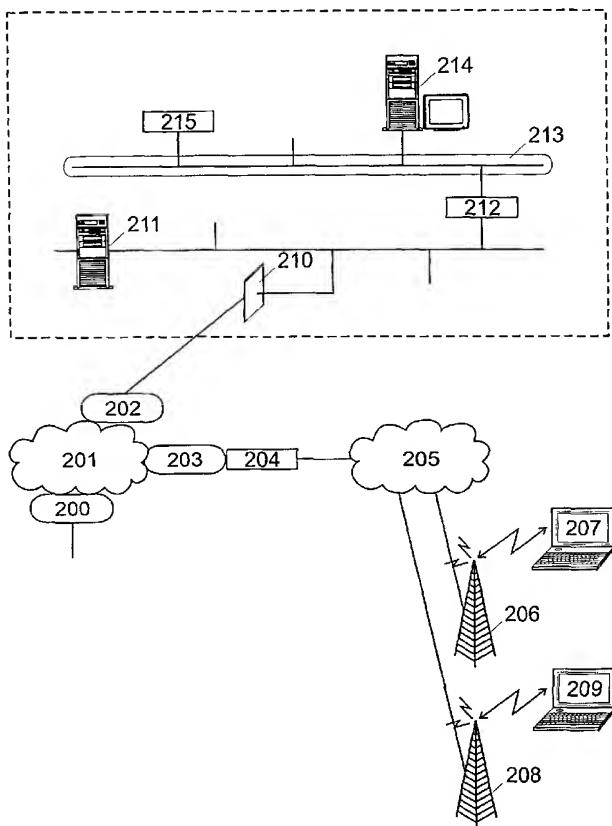
(26) Publication Language: English

(30) Priority Data:
60/181,090 8 February 2000 (08.02.2000) US

(72) Inventors; and
(75) Inventors/Applicants (for US only): FERCHICHI, Azim

[Continued on next page]

(54) Title: SINGLE SIGN-ON PROCESS



(57) Abstract: Single sign-on process allowing a mobile user with a mobile phone or with a laptop to remote-access a remote server, comprising the steps of: (1) sending a first authenticator over a first communication layer to a first intermediate equipment between said mobile equipment and said remote server, (2) verifying in said first intermediate equipment said first authenticator sent by said mobile equipment, (3) if said first authenticator is accepted by said first intermediate equipment, completing the communication layer between said mobile equipment and said intermediate equipment, (4) repeating steps (1) to (3) with a plurality of successive intermediate equipment and over a plurality of successive communication layers, until a communication has been completed at the last requested communication layer between said mobile equipment and said remote server, wherein at least a plurality of said authenticators are furnished by a smart-card in said mobile equipment.

WO 01/60013 A1



(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Single sign-on process

The invention concerns a single sign-on process and a smart-card used for said single sign-on process.

The present invention also concerns a process for changing a 5 secret from a plurality of equipment in a network.

1 - Related Art

When users remote-access a corporate network or a private LAN, various communication layers have to be built-up. Generally, each layer requires an authentication. For each authentication, the users may enter 10 secrets, for example a PIN, a password, a passphrase or biometrics data. This leads to two problems. The more secrets the users have to remember, the more they tend to choose easy secrets and the more they tend to write them down. In addition, they also tend to forget them, which increases management costs.

15 One purpose of the invention is to use only one secret that serves for all authentications.

Single sign-on processes have already been proposed for users who want to log onto different machines, each having its own operating 20 system and its own type of authentication. This type of known single log-on process only works once all necessary communication layers have already been built. More specifically it is generally assumed that machines are inside a corporate network with TCP/IP as the basic communication layer.

Another purpose of the invention is to provide a single sign-on 25 process with an authentication that is not tied to machine log-on, but to layer construction. This means that each time a new layer has to be built-up, it may require a new authentication of the user or his/her machine.

Another purpose of the invention is to propose a single sign-on process that can be used for building a communication over different communication layers of different network protocols.

Known single sign-on systems are based on central servers on which the users make their first log-on. This approach is not practicable when the user does not have the required communication layers to contact the central authentication server. Another problem is that for each authentication required, we do not necessarily deal with the same company, and having one central server for all may lead to political and trust problems.

10 **2 - Summary of the invention**

In accordance with one embodiment of the present invention, those problems are solved with a process comprising the steps claimed in claim 1.

15 More specifically, those problems are solved with a single sign-on process allowing a mobile user with a mobile equipment to remote-access a remote location, comprising the steps of:

(1) sending a first authenticator over a first communication layer to a first intermediate equipment between said mobile equipment and said remote location,

20 (2) verifying in said first intermediate equipment said first authenticator sent by said mobile equipment,

(3) if said first authenticator is accepted by said first intermediate equipment, completing the communication layer between said mobile equipment and said intermediate equipment,

25 (4) repeating steps (1) to (3) with a plurality of successive intermediate equipment and over a plurality of successive communication layers, until a communication has been completed at the last requested communication layer between said mobile equipment and said remote location,

wherein at least a plurality of said authenticators are furnished by a smart-card in said mobile equipment.

According to an aspect of the invention, every step of the single sign-on process is carried out on the client side, preferably in a smart-card.

5 This process is advantageous in that it does not weaken any existing authentication mechanism already in place. Moreover, the use of a smart-card improves the overall security. No central single sign-on server is needed.

10 According to another aspect of the invention, one and only one password (or PIN, or biometric data, or any other secret) is entered by the user, e.g. by a mobile user, to remote-access an enterprise network, regardless of the number of authentications to be performed and regardless of the number of communication layers to be built up.

15 The inventive process allows for a transparent layer construction and transparent user or machine authentication at each layer. Layers can be transparently reconstructed in case of unintentional communication cut-off.

Brief description of the drawings

Fig. 1 shows the general concept of the inventive process.

20 Fig. 2 illustrates the definition of an authenticator in an authentication scheme.

Fig. 3 illustrates a hashed authentication mechanism.

Fig. 4 illustrates a cryptographic authentication mechanism without key protection.

Fig. 5 illustrates a symmetric cryptographic authentication mechanism with weak key protection.

Fig. 6 illustrates a symmetric cryptographic authentication mechanism with strong key protection.

5 Fig. 7 illustrates an asymmetric cryptographic authentication mechanism with strong key protection

Fig. 8 illustrates an authentication process for a permanent secret authentication mechanism.

10 Fig. 9 illustrates the authentication process for a hashed password authentication mechanism.

Fig. 10 illustrates an authentication process for a symmetric authentication mechanism without key protection or with weak key protection.

15 Fig. 11 illustrates an authentication process for a symmetric authentication mechanism with strong key protection.

Fig. 12 illustrates an authentication process for an asymmetric authentication mechanism.

Fig. 13 illustrates the interaction between the components used for the single sign-on process.

20 Fig. 14 shows a dataflow illustrating the process steps executed for the layer construction in an embodiment of the inventive process.

Fig. 15 illustrates a system comprising a GSM network, a PPP part, an IPSEC part and a NT part, in which the inventive process can be used.

Fig. 16 shows how the layers are constructed in the system of Figure 15.

Fig. 16a illustrates the layer construction according to the inventive process.

5 Fig. 17 illustrates the GSM authentication mechanism.

Fig. 18 illustrates the authentication mechanism for PAP two-way handshake.

Fig. 19 illustrates the authentication mechanism for PAP integrating a smart-card.

10 Fig. 20 illustrates the authentication mechanism for CHAP integrating a smart-card.

Fig. 21 illustrates the authentication mechanism for EAP using OTP integrated with a smart-card.

15 Fig. 22 illustrates the message exchanges during IKE (Internet Key Exchange) main mode.

Fig. 23 illustrates the message exchanges during IPSEC quick mode.

Fig. 24 illustrates the authentication mechanism for NT.

20 Fig. 25 illustrates the process steps of a secret synchronization process which is performed when a secret change has been requested by the operating system.

Fig. 26 illustrates the process steps of a secret synchronization process which is performed when a secret change has been requested by the user.

Figure 1 shows a schema illustrating the general concept of the invention. The reference number 13 shows a single sign-on module, which can include hardware and software parts. The single sign-on module can be realized as a software module running on a microprocessor in a mobile equipment of a user 10. It includes a smart-card interface for interconnecting over an API interface with a smart-card 17. Reference numbers 22, 23, 10 .., 2i, .. 27 show superposed layers of a telecommunication protocol stack.

All process steps are initiated by the single sign-on module 13. When the user requests a remote access with his corporate network, the single sign-on module 13 launches the user interface (arrow 11) in order to prompt the user for his login name and secrets. This step may include 15 displaying a dialog box on a graphical user interface on the display of the user equipment, a voice prompt, etc. The user 10 then enters his login name and passwords (arrow 12). The secrets may include a password, a passphrase, user biometrics data, etc.

The login name and the secrets entered are then checked in the 20 single sign-on module 13 and compared with names and secrets stored in a protected memory area of the module 13 (not shown) to verify the user's authorization. If the test fails, the user may be requested to try again, until a predefined maximal number of tries has been reached. Otherwise, the 25 smart-card 17 is activated (arrow 15) in order to retrieve the login information (arrow 16) needed for successively completing the communication layers 22-27 (arrows 18-21).

3 - General theoretical description

We will now introduce a few definitions and theoretical concepts that will be needed in the following sections.

3.1 - Classification of authentication mechanism

3.1.1 - Definition

Figure 2 shows a sender 30 and a receiver 36. The receiver 36 gives the sender access to the requested services only if an authenticator 37 received from the sender can be verified. The authenticator 33 sent by the sender is processed using processing means 34 from a secret 31 entered by the user, e.g. from a password, a passphrase, a PIN or biometrics data, and from other data 32, such as the user ID, the time, etc. The authenticator is defined as being the raw data that is received by the receiver 36 in an authentication scheme and that will be used to verify the identity of the sender 30. This authenticator is sent over a communication channel between the sender and the receiver (arrow 35) and verified in a verification process 39 by the receiver 36, in order to deliver an authentication result 38.

The verification process 39 and the receiver 36 can use different kinds of authenticators 37:

3.1.3 - Clear-text authenticators

In this category, no processing is made to transform the secret 31 entered by the user 10 in a non-readable form. This implies that we can directly read the secret entered by the user by reading the authenticator.

3.1.3.1 - Permanent secret (Mechanism AUTH1)

In a first case of clear-text authentication mechanism, which will be denoted as the mechanism AUTH1, the same secret 31 included in the authenticator serves to perform many authentications. A typical example is remote login on most UNIX machines. The user always types the same password and the password is sent in clear text to the machine. This type of authentication is the weakest one.

3.1.3.2 - One-time secret (Mechanism AUTH2)

In a second case (AUTH2), a new secret 31 is entered by the user 10 each time a new authentication is required. For example, the user can be provided with a list of passwords or PINs that he has to keep secret. The 5 receiver 36 also has to have the same list. At each new authentication, the user takes the next password on the list and sends it in clear text to the receiver for verification.

Another known example is the so-called SecureID authentication process. In this case, the user 10 is provided with a token that display a new 10 secret number each minute. At each authentication the user enters the new displayed number.

This type of authentication provides protection against replay attack. However, it shall be implemented in such a way that it shall not be possible to guess the next coming password or PIN, even if an attacker has 15 all the previous ones.

3.1.4 - Cryptographic authenticators

In this category, the secret 31 entered by the user 10 is converted in a non-readable form using a cryptographic function.

3.1.5 - Hashed password (Mechanism AUTH 3)

20 This category of cryptographic authentication mechanism is illustrated in Figure 3. In this case, a one-way hash function 51 is used to transform the secret 50, together with some other data such as a replay attack protection, the user-ID, a sequence number or a random number, in an encrypted authenticator 52.

25 The hash function is an algorithm that takes a variable length input and produces a fixed length output. A hash function is considered a

secure transformation function if it fulfils the following characteristics: the output is a fixed length string even if the input is a variable length string; they have to be one-way functions, i.e. given an output it is not possible to guess the input; they have to be collision-free, i.e. it is hard to generate

5 two inputs that give the same output. These functions are generally referred to as one-way hash functions. Example of such functions are: Snefru, N-Hash, MD4 (Message Digest 4), MD5 (Message Digest 5), MD2 (Message Digest 2), SHA Secure Hash Algorithm), Ripe-MD, Haval, etc.

In this type of mechanism, the password as input is generally

10 concatenated with other information, etc.

3.1.5.1 Symmetric algorithms

3.1.5.1.1 Symmetric algorithms without key protection (Mechanism AUTH4)

This case is illustrated in Figure 4. In this case, a cryptographic

15 function 62 is used with a key 61 to transform the data 60, including the user secret and a replay attack protection, such as a user-ID, a sequence number or a random number, in an encrypted authenticator 63.

In this scenario, the key 61 used by the cryptographic function 62

20 is only protected at operating system level. In other words, it means that the secret key is stored on the disk in clear text format, and its access is only protected by operating system access control. Hereafter, some examples of symmetric cryptographic functions: DES, Triple DES, IDEA, REDOC, MMB, etc.

3.1.5.1.2 - Symmetric algorithms with weak key protection (Mechanism AUTH5)

This case is illustrated in Figure 5. In this case, a secret 64 must be entered by the user in order to get access (arrow 65) to an application or

software 66 with which some data such as a replay attack protection, the user-ID, a sequence number or a random number, etc, can be encrypted by a symmetric cryptographic function 63 using a secret key 68. The function 63 computes an encrypted authenticator 70.

5 It gives a weak protection, because the secret key 68 can still be accessed at operating system level, since it is stored on the disk in clear-text form.

3.1.5.1.3 - Symmetric algorithms with strong key protection (Mechanism AUTH6)

10 This case is illustrated in Figure 6. In this scenario, the secret key 92 is directly derived from the secret 90 (PIN/password) entered by the user, using a secure transformation function 91. This key is used by a symmetric cryptographic function 94 to compute the encrypted authenticator 95 from the replay attack protection data 93. Thus, the secret key 92 is never stored
15 on the client hard-disk. These secure transformation functions are the same as the one-way hash functions described above and have the same characteristics.

3.1.5.2 Asymmetric algorithms

3.1.5.2.1 Asymmetric algorithms without key protection 20 (Mechanism AUTH7)

The scenario is the same as the one described in §3.1.5.1.1 in connection with symmetric algorithms without key protection, except that the secret key has to be replaced by the private key.

25 Example of asymmetric algorithms include RSA (Rivest Shamir Adleman), ECC (Elliptic Curve Crypto-system), El-Gamal, DSA, ESIGN, etc.

3.1.5.2.2 - Asymmetric algorithms with weak key protection (Mechanism AUTH8)

The scenario is the same as the one described in §3.1.5.1.2 in connection with symmetric algorithms with weak key protection, except
5 that the secret key has to be replaced by the private key.

3.1.5.2.3 - Asymmetric algorithms with strong key protection (Mechanism AUTH9)

This case is illustrated in Figure 7. In this scenario, the private key 105 used by the asymmetric cryptographic function 107 to calculate the
10 authenticator 108 from the data 106 is itself protected. It is stored in an encrypted form on the client hard disk. To decrypt it, a password/PIN 100 has to be entered. A secret key 102 is derived from this password 100 with a secure transformation function 101; this secret key 102 is used by the symmetric decryption module 103 to decrypt the private key 104. The
15 secure transformation function is a one-way hash function.

3.2 - Integration of authentication mechanisms with the smart-card

3.2.1 - Authentication data and authentication functions

We will now describe, for each authentication type described
20 above, what authentication data will be stored in the smart-card 17 of the invention, and what authentication functions need to be implemented in the single sign-on module 13.

Most of the time the AUTH2 type of mechanisms are working with external and standalone devices (either a token displaying the
25 PIN/password or a paper sheet on which the PIN/passwords are written down), and it is often undesired to implement them on a smart-card. For

this reason, this type of mechanisms will not be described any further in this document.

3.2.2 - Authentication mechanism using the smart-card

Figure 8 shows the authentication process for type AUTH1

5 authentication (Clear-text authenticator). In this case, the smart-card 17 just serves as a secure repository for authenticators. When the single sign-on module requests a login from an authentication server 110 of the type AUTH1 (arrow 113), the latter replies by requesting an authenticator, usually a PIN or a password (arrow 114). The single sign-on module 13 requests 10 this authenticator from the smart-card (arrow 111). If the latter is in active state, it sends the authenticator to the module 13 (arrow 112), possibly with other data. This authenticator is transmitted with other data to the server 110 (arrow 115); if the authenticator is verified, it sends the authentication results to the single sign-on module 13 (arrow 116).

15 Figure 9 shows the authentication process for AUTH3 type authentication (Cryptographic authenticator). In this case, the smart-card 17 is used to securely store the secret and to calculate the hash value derived from the stored secret. When the single sign-on module requests a login from an authentication server 127 of the type AUTH3 (arrow 122), the 20 latter replies by requesting an authenticator, usually the hash value of a PIN or password (arrow 123). The single sign-on module 13 requests this authenticator from the smart-card (arrow 120). If the latter is in active state, it computes the authenticator from the user password and possibly from other data and sends it to the module 13 (arrow 121), which sends it 25 to the server 127 (arrow 124); if the authenticator is verified, the server 127 sends the authentication results to the single sign-on module 13 (arrow 125).

Figure 10 shows the authentication process for AUTH4 (symmetric algorithms without key protection) and AUTH5 (symmetric algorithms with

weak key protection) type authentication. In this case the smart-card 17 securely stores the secret key.

When the single sign-on module 13 requests a login from an authentication server 136 of the type AUTH4 or AUTH5 (arrow 132), the 5 latter replies by requesting an authenticator (arrow 133). The single sign-on module 13 sends the data for authentication to the smart-card (arrow 130). If the latter is in active state, it encrypts the data using symmetric algorithm with the secret key to produce the authenticator which is sent to the single sign-on module (arrow 131) that forwards it (arrow 134) to the authentication server 136 for verification; if the authenticator is verified, the server 10 136 sends the authentication results to the single sign-on module 13 (arrow 135).

Figure 11 shows the authentication process for AUTH6 type authentication (Symmetric algorithms with strong key protection). In this 15 case, the smart-card 17 securely stores the password.

When the single sign-on module 13 requests a login from an authentication server 140 of the type AUTH6 (arrow 143), the latter replies by requesting an authenticator (arrow 144). The single sign-on module 13 requests the authenticator (arrow 141). The smart-card 17 first derives the 20 secret key by applying a secure hash function over the secret (password/ PIN). Then it encrypts the data with the secret key previously derived using a symmetric cryptographic function scf, and gives out the authenticator to the single sign-on module (arrow 142) which transmits it (arrow 145) to the authentication server 140 for verification; if the authenticator is verified, 25 the server 140 sends the authentication results to the single sign-on module 13 (arrow 146).

Figure 12 shows the authentication process for AUTH7 (asymmetric algorithms without key protection), AUTH8 (asymmetric algorithms with weak key protection) and AUTH9 (asymmetric algorithms with strong

key protection). In this case the smart-card stores the private key that serves to asymmetrically encrypt the data to produce the authenticator.

When the single sign-on module 13 requests a login from an authentication server 150 of the type AUTH7, AUTH8 or AUTH9 (arrow 153), the latter replies by requesting an authenticator (arrow 154). The single sign-on module 13 requests the authenticator (arrow 151). The smart-card 17 encrypts the data with the private key, using a secure transform function stf and/or a symmetric cryptographic function scf and sends the authenticator to the single sign-on module (arrow 152), which forwards it to the authentication server for verification (arrow 155); if the authenticator is verified, the server 150 sends the authentication results to the single sign-on module 13 (arrow 156).

The table 1 below resumes the smart-card storage and processing function for each kind of authentication mechanism:

Smart-card Storage and processing			
Types of authentication mechanism	Cryptographic keys	Secret	Secure Functions
AUTH1	-	Password or PIN	-
AUTH2	Secret key	-	Symmetric cryptographic function
AUTH3	-	-	hash function
AUTH4	Don't apply	Don't apply	Don't apply
AUTH5	Secret key	Password or PIN	Card activation function using PIN/password Symmetric cryptographic function
AUTH6		PIN/password	Secure transformation from PIN/password to secret key Symmetric

			cryptographic function
AUTH7	Private key, Public key		Asymmetric cryptographic function
AUTH8	Private key, Public key	PIN/password	Card activation function using PIN/password Asymmetric cryptographic function
AUTH9	Private key, Public key	PIN/password	Secure transformation from PIN/password to secret key Decryption of private key using secret key derived from PIN/password Asymmetric cryptographic function

The table above shows a one-to-one mapping of the existing mechanisms into the smart-card 17. However, thanks to the properties of the smart-card, the mechanisms AUTH9 can be optimized or simplified without weakening these authentication mechanisms.

5 The smart-card to be used is preferably a secure smart-card. It has preferably the property to be tamperproof, i.e. it has to resist to all known types of hardware attacks.

10 In addition, software stored in a smart-card is usually composed of two parts: one stored in ROM, generally called the operating system (OS), and the other one stored in EEPROM, generally called the application. The OS and the application stored in a smart-card are so small and restrictive that it is possible to guarantee that some chosen data will never be read out.

15 While with a computer (and especially with a laptop), it is generally impossible to guarantee that the security provided by the OS will not be bypassed and that some secret data will be read out by an unauthorized

person, with a smart-card we can assume that the security system will not be bypassed.

Based on the assumptions made above, there is no need anymore to store the private key of AUTH9 in an encrypted form in the memory of 5 the smart-card.

Thus AUTH9 can be simplified and becomes the same as AUTH8, without decreasing its level of security.

If we refer to table 1, except AUTH3 and AUTH6 all secrets (PIN/passwords) are not directly involved in the calculation of the authenticator 10 but only to protect the access to the calculation of the authenticator. Instead of having one secret for each system, we can define one secret at the smart-card level that protects the access to all types of authenticator calculations. The secret used to get access to the smart-card is called card activation secret or card activation PIN/password.

15 3.3 - Overall processing

We will now describe with Figure 13 how the inventive single sign-on process works. The user 10 is prompted by the single sign-on module 13 at the beginning to enter a login name and a secret (PIN/password/ biometrics) on a graphical user interface 160. This secret is used to 20 activate the smart-card 17, and thus the smart-card will be able to process all authentications required thereafter for each layer. An external interface 161 forwards the authentication requests from the various authentication servers 162 to 169 to the single sign-on module 13, and sends back the retrieved authenticator from the smart-card 17 to those servers.

25 The authentications are performed only if the smart-card 17 is in an active state. To be in such a state two conditions are mandatory: the smart-card must first be powered-on; then the correct activation secret must be given. When the smart-card is powered-off (i.e. removed from its

reader), it automatically returns in an inactive state. Thus, a stolen card becomes unusable for an attacker.

Figure 14 shows the sequences of processes for the inventive single sign-on process for multi-layering authentication using a smart-card.

5 After the boot of the machine, the single sign-on (SSO) module 13 launches the graphical user interface (step 170) and prompts the user 10 for the login name and secret. The user may choose not to do the single sign-on and types cancel, e.g. when using the machine in a standalone mode (step 171). In this case, there is no remote login (step 172).

10 If the user 10 decides to enter a login name and secret (step 177), the single sign-on module transmits them during step 178 to the smart-card 17 for verification. If the smart-card is powered on, it verifies these data during step 179. When the login information provided is incorrect, the smart-card increases an internal counter (step 180). If its value is greater 15 than a threshold value (test 173), then the card blocks itself to become unusable (step 174) and sends the login results to the single sign-on module 13 (step 175). The login has failed (step 176).

20 The authenticator used for the authentication of the user 10 may use biometrics parameters, e.g. fingerprints, iris pattern, retina pattern, voice parameters, face parameters, etc.

25 For example, the threshold value can be set to 3, permitting the user to try three times a log-on. This mechanism is implemented in the card, to prevent an attacker to do a brute force attack on the card i.e. trying all possible combinations of secrets until finding the one matching. Of course the counter is reset to 0 each time the user 10 has provided the right secret only if the card is not already blocked.

If the login information is correct, then the smart-card 17 turns itself into an active state (step 181) and acknowledges the single sign-on

module (step 182). The latter can start to build the different communication layers (steps 183 to 184). Starting from the lowest level, it checks during step 185 if it requires an authentication for the establishment of the communication. If no authentication is required, the communication 5 layer is automatically built-up during step 186.

If an authentication is required, then the remote authentication server sends the necessary data (if needed) to the single sign-on module 13. The single sign-on module transmits these data to the smart-card 17. The smart-card then returns the authenticator to the single sign-on module 10 (step 188). This authenticator is then transmitted to the remote authentication sever for verification (step 190). The authentication server can perform the authentication itself, or delegates the verification of the corresponding authenticator to a third equipment (not shown). If the authentication is not valid, the authentication may be repeated a certain number of times using 15 the counter value a, and then, if still wrong (test 191), stopped either by the remote server or by the single sign-on module (step 192). If the authentication is correct, the communication layer set-up is completed (step 186). The single sign-on module 13 proceeds the same way with other layers L_i , until all i_{max} layers are completed (incrementing step 193).

20 3.4 - Transparent layer reconstruction

If, for any reason, one communication layer loses the connection, the single sign-on module 13 shall be able to rebuild the layer without user intervention. In this case, the single sign-on module 13 preferably verifies that the smart-card 17 is still present and in an active 25 state. Then it has to send a new authenticator to the authentication server. The authentication procedure then proceeds as described above.

4 - Embodiment using GSM, PPP, IPSEC and NT

4.1 - A new emerging remote access service

We will now describe in more detail an embodiment of the inventive process in which a communication is built between the client 10 and a remote server through GSM (Global System for Mobile), PPP (Point To Point Protocol), IPSEC (Internet Protocol Security) and Windows NT (New

5 Technology; Trademark of Microsoft Corp.) network layers.

New terminals with high data rate (43,2 kbits/s and higher) dedicated to mobile telephony are coming onto the market. They integrate a GSM phone, a GSM SIM card, and support HSCSD (High Speed Circuit Switched Data), GPRS (General Packet Radio Service), EDGE (Enhanced Data 10 for GSM Evolution) and/or UMTS (Universal Mobile Telecommunications System) technology for high speed communication. These terminals may be inserted in the slot of laptop just as a PC Card type II or type III, or be integrated in a mobile phone or personal digital assistant (PDA).

These terminals allow a fast access to remote locations without 15 using the fixed telephone networks. Instead, the GSM network is used until the first ISDN (Integrated Services Digital Network) or PSTN (Public switched Telephone network) router. However, remote access presents different security risks as it might cross unprotected or public networks. IPSEC is a security protocol at IP (Internet Protocol) level that permits to guarantee a 20 good level of security from the laptop to the point of entry of the remote network (generally called gateway). Finally, when mobile users try to connect to their corporate network, it is likely that they log onto their NT domain.

For such a remote access, many layers are built up progressively 25 and normally each of them requires an authentication of the mobile user or of the machine that acts on behalf of the user. We will see hereafter how these different authentications may be performed with only one login action from the mobile user, using a smart-card.

4.2 - Layers construction

This situation is illustrated in Figure 15. A plurality of mobile users 207, 209 use mobile equipment such as a laptop computer, a personal digital assistant or a mobile phone to access data files and applications in a remote NT server 214 of their corporate network 213. The communication 5 is established through a basis station 206 respectively 208 of a GSM network 205 and the internet 201 via an internet service provider 203 using a router 204. The NT server 214 is connected to the Internet 201 via the corporate LAN 213, a router 212, an IPSEC gateway 211, a firewall 210 and another internet service provider 202. Other routers 215 may be connected 10 to the corporate network 213 to provide access to other networks and sub-networks. Other internet service providers 200 provide access to the Internet 201.

Figure 16 illustrates the layer construction in this specific embodiment of the invention. Elements and process steps equivalent to 15 those already described in connection with Figure 1 are designated with the same reference numbers and will not be described again. The single sign-on module 13 is shown here as a part of a middle-ware 210, e.g. a mobile equipment, a laptop, a palmtop, etc. The user 10 can access a remote server by constructing at least the following successive network 20 layers:

- a GSM layer 215, which requires a GSM authentication 211,
- a PPP layer 216, which requires a PPP login with a CHAP authentication 212,
- an IPSEC layer 217, which requires an IPSEC authentication 213,
- an NT layer 218, which requires a NT login 214.

25 We will now describe the construction of those four layers.

4.2.1 - GSM

The GSM layer 215 provides three security services: subscriber identity authentication, user and signaling data confidentiality, and subscriber identity confidentiality.

- 5 The first service is used to establish the identity of the mobile subscriber (MS) when he is trying to access the GSM network. The authentication is initiated by the fixed network 231 (Figure 17) that sends a challenge 234 (random number) to the mobile phone 230. This challenge is forwarded to the smart-card 17, also called SIM (Subscriber Identity
- 10 Module) card in this context, which computes the response 233 by applying the A3 one-way hash function to the random number received with the secret key stored in the smart-card and with the user identification. This answer is forwarded to the network (arrow 235), which verifies it and acknowledges a success or a failure (arrow 236).

- 15 The secret key 17 used for computing the hashed value is shared only by the smart-card and an authentication center, which serves the subscriber's home network. The output of the hash computed by the SIM card 17 is transmitted to the fixed network 231, where it is compared with a pre-computed value. If the two hash values match, the user (mobile
- 20 subscriber) has been authenticated, and the call is allowed to proceed. If the values are different, then access is denied. If the card has not been set in an active state (i.e. correct PIN entered), this authentication cannot occur.

4.2.2 PPP

- 25 The next layer uses the Point-to-Point Protocol (PPP), which provides a standard process for transporting multi-protocol datagrams over point-to-point links. With PPP different authentication processes are possible:

- PAP (password authentication protocol), which uses a clear-text password,
- CHAP, which uses a MD5 one-way hash function,
- EAP, which uses a MD5 one-way hash function or OTP,
- 5 ▪ SecureID

4.2.2.1 - PAP

The PAP (password authentication protocol), which is illustrated in Figure 18, provides a simple process for a user 253 to establish its identity using a 2-way handshake with a remote server 256. This is done only upon 10 initial link establishment.

After the Link Establishment phase is complete, an ID/Password pair 254 is repeatedly sent by the client to the authentication server until authentication is acknowledged (arrow 255) or the connection is terminated.

15 PAP is not a strong authentication process. Passwords are sent over the circuit in clear-text format, and there is no protection against replay or repeated trial and error attacks. The user 253 is in control of the frequency and timing of the attempts.

This authentication process is of type AUTH1 as defined above.
20 To integrate PAP with the smart-card 17, the ID and password shall be stored in the EEPROM of the smart-card. When the single sign-on module 13 initiates a PPP link with the remote server 260 (Figure 19), it has to send an ID/password retrieve request (arrow 261) to the smart-card and to forward the answer 262 as an 'authenticate request' message 263. The 25 remote server 260 answers with an authenticate acknowledge or no-acknowledge message 264.

4.2.2.2 - CHAP

CHAP (Challenge-Handshake Authentication Protocol) is another widely used authentication process used by PPP. CHAP is used to periodically verify the identity of the user using a 3-way handshake. This is 5 done upon initial link establishment, and may be repeated anytime after the link has been established.

The integration of CHAP with the smart-card 17 is shown in Figure 20. After the Link Establishment phase is completed, the authentication server 275 sends a challenge message 272 to the single sign-on 10 module 13 of the user, which forwards it to the smart-card 17 (arrow 270).

The latter computes a hash value using the MD5 algorithm. This 15 MD5 algorithm will use as input the ID (stored in the smart-card) concatenated with the password (stored in the smart-card) and concatenated with the challenge (issued by the server). The result 271 is sent to the single sign-on module 13, which forwards it to the server 275. The server checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged (arrow 274); otherwise the connection is terminated.

20 CHAP provides protection against replay attack through the use of an incrementally changing identifier and a variable challenge value. The authentication server is in control of the frequency and timing of the challenges.

This authentication process is of type AUTH3 as above defined.

25 4.2.2.3 - EAP

The PPP Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication, which supports multiple authentication

mechanisms. After the link establishment phase, the authentication server sends one or more requests to the user. In these requests the server asks for the type of authentication it desires (MD5, OTP- One Time Password-, etc.). The user can either acknowledge with a response packet including the

- 5 authentication response, or denies the types of authentication proposed. The server has to propose other mechanisms until one matches. The MD5 authentication proposed in EAP is equivalent to a CHAP authentication, so its integration with a smart-card is the same as for CHAP. In the OTP authentication mechanism, a one-way hash function is also used, but it is
- 10 applied multiple times. In addition in OTP, we have the choice among at least three hash algorithms, namely MD4, MD5 and SHA1. Nevertheless, this authentication process is of type AUTH3 as defined above and its integration with a smart-card will follow the principle defined.

After the link establishment, the authentication server 280

- 15 (Figure 21) requests an authentication, specifying the type (arrow 283). If MD5 is requested, the principle is the same as described for CHAP. If OTP is requested, the authentication server sends in the request, the algorithm required and the seeds (kind of random number). The single sign-on module 13 of the user forwards the seed and the algorithm type to the
- 20 smart-card 17 (arrow 281). The smart-card 17 takes the OTP passphrase stored in its EEPROM, concatenates it with the seed received, then passes it through the hash algorithm selected. This first output is then passed n times through the hash algorithm. The final output 282 is then sent to the single sign-on module that transmits this result to the authentication server 280 through a PPP EAP response message 284. The result is checked by the authentication server that sends a PPP EAP success or failure message 285.

4.2.3 - IPSEC

4.2.3.1 IPSEC basic description

The IPSEC layer 216 uses the IPSEC protocols, which have been designed to provide secure channel between peers at IP level. Authentication, integrity, confidentiality and key exchange are provided.

An IPSEC packet has the following structure:

5 AH | ESP

wherein AH is an authentication header
and ESP is an encapsulating security Payload

AH provides connectionless integrity, data origin authentication using symmetric cryptographic algorithms, and replay protection thanks to
10 a digital signature over a sequence number.

ESP provides data privacy (or confidentiality) using symmetric cryptographic algorithms, plus AH security services.

For key exchange, IPSEC uses IKE (Internet Key Exchange). It describes a framework in which IPSEC connections can negotiate
15 authentication, encryption and key management information.

IKE is divided in two phases: the Main mode and the Quick mode. In the main mode, which is illustrated in Figure 22, an IKE Security Association (IKE SA) is defined. It contains all necessary information for two entities to exchange secured messages. In the Quick mode an IPSEC SA is
20 derived from the IKE SA to negotiate the keys for use with an AH and ESP.

The first message exchange is the negotiation of parameters. The initiator 290 proposes different algorithms for encryption and authentication, an expiry time and other parameters (arrow 292). The responder 291 has to choose one option for each parameter and transmit
25 its response 293.

In the second message, exchange nonces and Diffie-Hellman public keys are transmitted. Nonces are random numbers, one (294) generated by the initiator and the other (295) by the responder. The particularity of Diffie-Hellman is that both parties can compute a secret key 5 only by exchanging DH public keys because:

$$DH = DH_{Public_I} \exp(DH_{Private_R}) = DH_{Public_R} \exp(DH_{Private_I})$$

The DH key calculated is used to encrypt the third message exchange. These messages 296, 297 contain a signature made with a private 10 key of each partner and an identification payload. This signature is applied over a hash. This hash is a function of the nonces, the Diffie-Hellman public keys, the negotiation parameters, the identification of the initiator (or responder) and the Identification payload.

$$\begin{aligned} \text{Hash_I} &= \text{fct}\{\text{nonce_I}; \text{nonce_R}; \text{DHpublic_I}; \text{DHpublic_R}; \text{parameters_I}; \text{ID_I}; \\ &\quad \text{etc.}\} \\ \text{Sign_I} &= \text{sign}(\text{Hash_I})_{K_{priv_I}} \end{aligned}$$

15

By verifying the signature, the responder can be sure of the identity of the initiator, and can be sure that the two previous messages were really sent by the initiator. In its turn, the initiator can verify the same about the responder.

20

In addition to the messages exchanged and the computation described above, three secret keys are generated. They are used for the next mode called quick mode. These keys are:

Skey_d: Secret key used to derive future keys

25 Skey_a: Secret key used to authenticate messages exchanged in quick mode

Skey_e: Secret key used to encrypt messages exchanged in quick mode

In the quick mode illustrated in Figure 23 random numbers are exchanged between the initiator 310 and the responder 311 during steps 5 312 and 313. Those numbers are used to generate new keys to be used to encrypt ESP and sign AH header of IPSEC packets.

The authentication in IKE main mode can be accomplished by different algorithms. In the message exchanged shown in Figure 22, we have illustrated only one type of authentication. Among the possible 10 authentication processes, IKE proposes a pre-shared secret using a symmetric algorithm, DSS signatures, RSA signature, Encryption with RSA and Revised encryption with RSA. Whether we use one authentication or other, the message exchanged might slightly differ while the principle remains the same.

15 4.2.3.2 Operations to be done in the smart-card

A considerable amount of keys is generated in the IPSEC protocol. In addition, a lot of encryption/decryption and signature operations are done. Only very powerful and expensive smart-cards can perform all these operations; most cheap smart-cards lack memory and 20 power processing.

Thus, we have to carefully choose which operations have to be performed by the smart-card 17.

The most critical key is the one used to perform the signature in the third message exchange 296, 297 of the main mode. Not only is this key 25 used to verify the identity of the initiator 290/responder 291, but it also serves to authenticate the first DH keys and nonce 294, 295 from which all the rest of the keying material is derived. In the case of the initiator 290 being represented by a laptop, if this key is compromised then any

communication with a gateway accepting this laptop is also compromised and more harmful, any access granted to this laptop is also granted to the attacker.

The smart-card 17 shall perform at least this signature operation
5 (if signatures are used for authentication; if other authentication processes are used, the equivalent operation shall be performed by the smart-card 17).

For the other operations, it is a trade-off between security and capacity (both processing and memory) of a smart-card. For example, we
10 can imagine generating the DH keys of the main mode in the smart-card; it is also possible to perform all the main mode in the smart-card (DH keys, hash calculation and signature over the hash).

Another point that is not mentioned in IKE, but that is present in most IPSEC implementation, is the certificate. Each time we use public key
15 systems we have to provide along with the public key a certificate. This certificate is generated by a trusted third party called CA (Certification authority). The certificate is in fact a signature by the CA over the public key of the Initiator/responder. It certifies that this public key really belongs to the Initiator/responder. This certificate may be stored in the smart-card,
20 or in a central server (e.g. in an X.500 directory).

4.2.4 - Windows NT layer

The SMB protocol is used in order to access the Windows NT layer
218 in a remote location, and a session authentication occurs to guarantee access control. The used dialect is negotiated between the client and the
25 server. Three possibilities can occur:

- Plaintext session authentication
- LanMan challenge/response session authentication

- NTLM challenge/response session authentication

Plaintext session authentication consists in simply sending the NT password in clear-text format to the authentication server called the PDC (Primary Domain Controller). This authentication is used with old Lan

5 Manager and SMB servers and should be avoided whenever possible.

LanMan challenge/response session authentication encrypts the challenge sent by the PDC using a key derived from the NT password. This key is called the LM hash and is explained below.

NTLM challenge/response session authentication encrypts the
10 challenge sent by the PDC using another key derived from the NT password. This key is explained below.

Both for LanMan and NTLM authentication, the client encrypts the challenge three times using DES algorithm, where each encryption uses a different section of the keys (LM hash or MD4-NT hash) as the source
15 material for the DES key. The ciphertext is returned to the PDC which then performs the same encryption process using its own copy of the users' password hashes from the SAM (Security Account Manager) database. If the client and server get the same results, the user is authenticated.

4.2.4.1 - LM Hash in Windows NT

20 The Lan Manager hash (LM Hash) is used in order to be compatible with older versions of Microsoft networking software. It can be found in the SAM of the primary domain controller PDC and a variation of it is sent on the network for remote authentication purposes. Note that it is now possible to avoid the LM hash to be sent on the network in a pure NT
25 environment (i. e. no Win 95 systems or other legacy).

The LM hash is generated by limiting the user's password to 14 characters padding with nulls if it is shorter, converting all characters to

ASCII uppercase, breaking the 14 characters (single byte OEM character set) into two 7 byte blocks, expanding each 7 byte block into an 8 byte DES key with parity, and DES ECB encrypting a known string with each of the two keys and concatenating the results.

5 4.2.4.2 - MD4-NT hash in Windows NT

The MD4-NT hash (often also called only NT hash) is created by taking up to 128 characters (in practice the NT password is limited to 14 characters by the GUI) of the user's password, converting it to unicode (a two byte character set used heavily in NT), and taking the MD4 hash of the 10 string, which produces 16 bytes called "NT password hash"; they are stored in the SAM database.

4.2.4.3 - Integration with smart-card

The Plaintext NT password authentication is of type Auth1.

The NTLM and LanMan authentications are both of type Auth6, 15 even if the LM hash doesn't use a pure hash function.

Figure 24 illustrates the dialogue exchange for a NT authentication performed with a smart-card 17. At negotiation, the type of NT authentication is asked by the single sign-on module on the client's side (arrow 334). If encrypted passwords are used, the primary domain 20 controller 13 sends a challenge to the single sign-on module (arrow 335). This challenge is forwarded to the smart-card 17 (arrow 331), which encrypts it using LM hash or NT hash as a key. These hash are derived from the NT cleartext password stored in the EEPROM of the smart-card, using transformation functions. The smart-card answers with a cleartext password 25 (arrow 332) or with an encrypted password (arrow 333), which is forwarded by the single sign-on module 13 to the PDC (arrow 336). The primary domain controller verifies the password and answers with a success or failure packet (arrow 337).

4.2.4.4 - Simple integration for NT

In the previous paragraph we have seen how to integrate the NT authentication with the smart-card following the general principle described above. However, for various reasons a simpler integration might 5 be judicious. First, to integrate the NT authentication as described above requires a modification of the Operating System. This might not be easy and recommended. In addition, the NT authentication may require too much space in the smart-card memory. Finally, the authentication mechanism of Windows 2000 is different from NT. The update to Windows 10 2000 and to subsequent operating systems is much easier to perform on a computer than on a smart-card.

Thus it is recommended, at least in a first phase, to keep the NT authentication processing on the laptop, but to store the NT password on the smart-card. The smart-card in this case just serves as secure NT password 15 storage, and each time an NT authentication is required, the smart-card gives the NT password to the OS (Win NT or Win95), through the single sign-on module, provided the smart-card is in an active state (i.e. powered on and correct activation PIN/password entered).

20 4.3 Summary of smart-card integration with GSM, PPP, IPSEC, NT

Figure 16a illustrates how a connection is established between the laptop 2 and the remote location 28 by successively constructing the successive superimposed network layers. The laptop first establishes a GSM connection with an internet service provider 12 via a mobile equipment 4 using a SIM-card 40, a public land mobile network 6, a home location 25 register 8 in this PLMN, and a router 10 connected to this HLR. The next PPP layer is constructed by authenticating the user 2 in the ISP, thus allowing access through the Internet 14 to a firewall 16 of the user's corporate network. If the user can be authenticated in this firewall, the next IPSEC

layer may be constructed, so that the user can access the requested domain in the server 26. A domain authentication is performed in this server in order to build the last protocol layer allowing the user to access the requested files in the remote location 28.

5 The table below summarizes the smart-card integration with
GSM, PPP, IPSEC and NT:

Layer	Authentication material	Authentication algorithm/function
GSM	Authentication key	GSM algorithm (A3, etc.)
PPP	PAP password	no processing
	CHAP password	MD5
	OTP passphrase	MD4 MD5 SHA1
IPSEC	Keys Certificate	Pre-shared secret algorithm DSS RSA signature RSA encryption RSA encryption revised
NT	NT Domain password	NTLM hash algorithm MD4-NT algorithm DES
NT (simple integration)	NT Domain password	no processing

This table summarizes what should be implemented in the smart-card in order to realize the authentications for the different layers
10 involved, namely GSM, PPP, IPSEC and NT. Keys and Passwords should be stored in the EEPROM of the smart-card. For the different cryptographic algorithms, the following guidelines may be followed: symmetric

algorithms should be coded in ROM; for asymmetric algorithms, a dedicated cryptographic coprocessor should be present in the smart-card.

It is obvious that before any authentication may take place, the smart-card shall be in an active state, i.e. the user shall enter the right
5 secret (PIN/password/biometrics).

GSM smart-cards (called SIM cards) already exist. The corresponding SIM software will be reused as it is in the smart-card that will integrate the single sign-on system.

As already described, we already have card phone devices that
10 integrate a SIM card and that can be plugged into the PC slot as a standard PC card. It is recommended to use the same card phone device to put in the single sign-on smart-card in place of the SIM card.

4.4 - Direct internal access and remote access compatibility

In the previous paragraph, we have seen how to implement a
15 single log-on for the authentications of each layer concerned (GSM, PPP, IPSEC, NT).

However, we will now explain here enhancements to what was presented before.

4.4.1 - Problem description

20 In the remote access service described, we are considering mobile users with laptops remote-accessing their corporate network. But it is likely that they also use their laptop while they are at their office. With the growing number of docking stations, users can easily use their laptop as their normal office computer directly connected to their internal corporate
25 network. In this situation there is no need anymore to have the card phone device, and users only have to log into their NT domain. To do this they will

have to use their NT password. However, in the description given, it is said that the user has only to remember the secret that makes the smart-card active, and then all the authentications are processed. In the case where the users also want to use their laptop directly as an internal machine (only 5 NT login), they have to remember a second secret in addition to the smart-card secret, namely the NT password.

In a single sign-on system we want to avoid having more than one secret to remember.

The simple solution is to make the NT password the secret to 10 activate the smart-card. Thus, the same secret can be used both for remote access single sign-on and for login to the NT domain for direct internal access.

Unfortunately, with such a solution another issue arises. If users 15 change their NT password when they are directly connected to their internal network, this new secret cannot be updated at the same time in the smart-card (because the card phone terminal containing the smart-card is not plugged in the PC slot). The next time users want to remote-log onto their network using the smart-card, the NT password stored in the DC will be desynchronized with the NT password stored in the smart-card. A 20 protected mechanism shall be implemented to ensure the secret synchronization.

4.4.2 - Solution: secret synchronization

The principle for the secret synchronization is the following:

If a user is directly connected to the internal network, the old 25 and the new NT passwords (secrets) are concatenated and encrypted with a synchronization public key stored in the PC. The next time the user logs in remotely, the two encrypted secrets are transmitted to the smart-card 17, which decrypts them using the corresponding synchronization private key

of the smart-card. Then, the old secret is compared with the one stored in the smart-card, and the new one is compared with the one entered by the user. If both results are correct, then the secret is updated in the smart-card and the building of the layers can proceed normally.

5 The processing for secret synchronization is depicted in Figure 25 and Figure 26, and explained in detail hereafter.

After the boot 350, the single sign-on module 13 of the laptop launches the login GUI (351). The single sign-on module detects that there is no smart-card (362) (i.e. the card phone terminal is not plugged in the PC slot), and prepares itself for the secret synchronization. When the user types in his/her NT secret (352), the single sign-on module keeps the NT secret in the laptop's RAM (361). In parallel, the normal NT domain login proceeds (353). If the NT domain secret previously entered by the user is not correct (test 354), the single sign-on module clears the secret stored in RAM (362) and restarts at 351. Note that the number of possible trials for NT secrets is generally determined by the password policy. If the NT secret entered by the user is correct, i.e. the NT domain authentication succeeds, then the user may be requested to change his/her secret (test 355). Note that this automatic secret change request is generally defined in the password policy. If no secret change request is required, the NT secret kept in RAM is cleared from this memory (363). Otherwise, the user has to enter his new secret (356). The single sign-on module intercepts this new secret, concatenates it with the old one previously kept in RAM (365). These two secrets are then encrypted with a public key (365). This public key will be further referenced as the synchronization public key.

The synchronization key pair is a pair of cryptographic keys to be used by an asymmetric encryption algorithm. Examples of asymmetric encryption algorithms include RSA, ECC, etc. The synchronization private key shall be stored on the EEPROM of the smart-card only, and it shall never be possible to read it out. One copy of the synchronization public key shall be stored on the laptop's disk. It is recommended to have a good

enough key length. For example if RSA is used, it is highly recommended to have a length of at least 1024 bits. For other algorithms, comparable strength should be used.

When the two NT secrets concatenated are encrypted, optional fields may be added with the secrets. Information such as date and time may be inserted; a sequence number and/or a random number may also be included. These parameters may enhance the security, in the sense that they render the secret encryption unique throughout time. Although replay attack may be difficult to realize and unlikely to succeed, such measures prevent these attacks.

The encrypted result is first stored in the laptop's RAM (366). If the NT secret change procedure (357) fails for any reason (test 358), the RAM is cleared (359), otherwise the result (2 encrypted passwords) is stored in a file on the laptop's disk (367). Appropriate measures should be taken to set minimum access permission to this file. Finally, an optional desynchronized state flag may be set (step 367), to further indicate to the smart-card that the two secrets are desynchronized.

Note that in the whole process described above, we assumed that the NT domain secret change was requested by the operating system. Obviously secret change may be initiated by the user, and this does not change the processes, except that the single sign-on module catches the 2 secrets at the same time (because users have to re-enter their old secret in addition the new one when they want to make a change).

The second part of the secret synchronization is realized when the user is using his/her laptop in remote access with the smart-card. This process is depicted in Figure 26 and the details are explained hereafter.

After the boot of the computer is completed (380), the single sign-on module launches the graphical user interface (381) for the user to log in. The user types in his/her NT domain secret and name (382). In the

meantime, the single sign-on module detects the smart-card presence in the computer slot (383). The single sign-on module checks then the desynchronized state (384). If there is no desynchronization, it means that the NT secret stored in the smart-card and the hash of the NT secret stored 5 on the operating system match. In this case the authentications and construction of the layers can proceed (385) as described above.

If we have a desynchronized state, then the single sign-on module starts to re-synchronize the secrets. It sends to the smart-card the encrypted information containing the two secrets plus the optional 10 information (386). It also passes to the smart-card the NT secret just typed by the user (387). The smart-card decrypts the information (388) using its synchronization private key stored in EEPROM. The smart-card can then extracts the old (391) and the new secret (389) as well as the optional 15 information (393). Three conditions should be met in order to proceed with the synchronization: the old NT secret extracted from the data decrypted has to be the same as the one previously stored in the smart-card (test 392); the new NT secret extracted from the data decrypted has to be the same as the one just typed by the user (test 390), finally the optional fields have to be correct (test 394). For example, if we have a sequence number in the 20 optional fields, the sequence number extracted from the data decrypted has to be greater than the one previously stored in the smart-card. If and only if all these conditions are fulfilled, then the smart-card can update the NT secret in its EEPROM with the new one (395). In addition, optional fields also have to be updated. If one of the above conditions is not met, then the 25 synchronization shall stop, i.e. no secret update shall occur. In addition, the smart-card and the single sign-on module should not proceed with the layer construction and corresponding authentication described above.

Otherwise, the smart-card informs the single sign-on module that the secret has been successfully updated. The single sign-on module deletes 30 the file with the encrypted data (the two secrets plus the optional fields), and resets its desynchronization state (396). Finally, the authentications and construction of the layers can proceed (397) as described above.

The one skilled in the art will recognize that this process of secret synchronization can be used for synchronizing any secrets between any pair or remote locations in a telecommunication network, independently from the described single sign-on process.

5 4.5 - Transparent layer reconstruction

It is likely that the GSM communication may be cut off. The single sign-on module should rebuild the layer without user intervention provided the user has not removed the terminal containing the smart-card from the PC slot.

Claims

1. Single sign-on process allowing a mobile user with a mobile equipment to remote-access a remote location, comprising the steps of:

5 (1) sending a first authenticator over a first communication layer to a first intermediate equipment between said mobile equipment and said remote location,

(2) verifying in said first intermediate equipment said first authenticator sent by said mobile equipment,

10 (3) if said first authenticator is accepted by said first intermediate equipment, completing the communication layer between said mobile equipment and said intermediate equipment,

15 (4) repeating steps (1) to (3) with a plurality of successive intermediate equipment and over a plurality of successive communication layers, until a communication has been completed at the last requested communication layer between said mobile equipment and said remote location,

wherein at least a plurality of said authenticators are furnished by a smart-card in said mobile equipment.

20 2. Single sign-on process according to claim 1, wherein at least one of said intermediate equipment delegates the verification of the corresponding authenticator to a third equipment.

25 3. Single sign-on process according to one of the claims 1 or 2, wherein said authenticators are delivered by said smart-card to a software module in said mobile equipment which sends it to said intermediate equipment.

30 4. Single sign-on process according to claim 3, wherein said software module initially prompts said user to enter his secret, and wherein said first authenticator is only sent if the secret entered by said user is correct.

5. Single sign-on process according to claim 4, wherein said secret is verified in said smart-card.
6. Single sign-on process according to claim 5, wherein said secret is the same as the secret requested for the domain authentication in said remote location.
7. Single sign-on process according to claim 1, wherein said mobile equipment comprises a cellular phone equipment.
8. Single sign-on process according to claim 7, wherein said smart-card is a SIM card.
- 10 9. Single sign-on process according to one of the claims 7 or 8, wherein said smart-card is a WIM card.
- 10 10. Single sign-on process according to one of the claims 7 to 9, wherein said first communication layer is a cellular mobile phone layer, said intermediate equipment being a fixed equipment in said cellular mobile phone system, and said first authenticator being used for authenticating said mobile user in said cellular mobile phone system.
11. Single sign-on process according to one of the preceding claims, wherein at least one of said authenticators is stored in said smart-card.
- 20 12. Single sign-on process according to one of the preceding claims, wherein at least one of said authenticators is computed in said smart-card.
- 25 13. Single sign-on process according to the preceding claim, wherein at least one of said authenticators is computed in said smart-card using a cryptographic function using at least one key.

14. Single sign-on process according to the preceding claim, wherein said cryptographic function uses a symmetric algorithm.

15. Single sign-on process according to the claim 13, wherein said cryptographic function uses an asymmetric algorithm.

5 16. Single sign-on process according to one of the claim 13 to 15, wherein said at least one key is stored in said smart-card.

10 17. Single sign-on process according to one of the preceding claims, wherein at least one of said communication layers is the internet, one of said intermediate equipment is an ISP server, and one of said authenticators is used by said ISP for verifying the identity of said user and granting him access to the internet.

15 18. Single sign-on process according to one of the preceding claims, wherein at least one of said communication layers is an IPSEC layer, one of said intermediate equipment is an IPSEC gateway, and one of said authenticators is used by said IPSEC gateway for verifying the identity of said user and granting him access to a network.

20 19. Single sign-on process according to one of the preceding claims, wherein at least one of said authenticators is used by said remote location for verifying the identity of said user and granting him access to a remote domain.

20. Single sign-on process according to one of the preceding claims, further comprising the steps of:
replacing a secret requested for accessing said remote location with a new secret in said remote location,
concatenating and encrypting the old and the new secret with a synchronization public key of said mobile equipment in said remote location,
entering the new secret in said mobile equipment,

transmitting the concatenated and encrypted old and new secrets to said mobile equipment,

decrypting said old and new secrets with a synchronization private key of said mobile equipment and corresponding to said

5 synchronization public key,

comparing said old decrypted secret with the secret stored in said mobile equipment, and comparing said decrypted new secret with said new secret entered in said mobile equipment,

if both comparisons are positive, replacing said secret stored

10 in said mobile equipment with said decrypted new secret, otherwise denying replacement of secret.

21. Process for replacing a secret in a plurality of equipment in a network, comprising the steps of:

replacing an old secret by a new secret in a first equipment,

15 encrypting the old and the new secret with a synchronization public key of a second equipment in said first equipment,

entering the new secret in said second equipment,

transmitting the encrypted old and new secrets to said second equipment,

20 decrypting said old and new secret with a synchronization private key of said second equipment and corresponding to said synchronization public key,

comparing said old decrypted secret with the secret stored in said second equipment, and comparing said decrypted new secret with said

25 secret entered in said second equipment,

if both comparisons are positive, replacing said secret stored in said second equipment with said decrypted new secret, otherwise denying replacement of secret.

22. Process according to the preceding claim, wherein said old

30 and new secrets are concatenated before encryption.

23. Process according to the preceding claim, wherein said second equipment is a mobile equipment.

24. Process according to one of the claims 21 to 23, wherein said synchronization private key is stored in a smart-card.

5 25. Process according to one of the claims 21 to 24, wherein
supplementary fields containing the date, time and/or the sequence
number are added to said encrypted old and new secrets.

26. Program storage device readable by a mobile equipment, tangibly embodying a program of instructions executable by the mobile equipment to perform process steps for authenticating the user of said mobile equipment, said process steps comprising:

prompting the user for a secret,
transmitting said secret to a smart-card in said mobile
equipment for verification,

15 if said secret is accepted by said smart-card, building a plurality of communication layers in order to connect to a remote location, every time that an authenticator is requested in order to complete a communication layer, asking said smart-card for said authenticator.

27. Smart-card that can be used in a mobile equipment for
20 authenticating the user of said mobile equipment, comprising processing
means for delivering a plurality of authenticators for authenticating said
user in a plurality of intermediate equipment at a plurality of communica-
tion layers between said mobile equipment and a remote location.

28. Smart-card according to claim 27, wherein said mobile
25 equipment comprises a cellular phone equipment.

29. Smart-card according to claim 28, which is a SIM card.

30. Smart-card according to claim 28, which is a WIM card.

31. Smart-card according to one of the claims 27 to 30, wherein at least one of said authenticators is stored in said smart-card.

32. Smart-card according to one of the claims 27 to 31, wherein at least one of said authenticators is computed in said smart-card.

5 33. Smart-card according to the preceding claim, wherein at least one of said authenticators is computed in said smart-card using a cryptographic function using at least one key.

34. Smart-card according to the preceding claim, wherein said at least one key is stored in said smart-card.

10 35. Smart-card according to one of the claims 27 to 34, wherein at least one authenticator can be used by an ISP for verifying the identity of said user and granting him access to the internet.

15 36. Smart-card according to one of the claims 27 to 35, wherein at least one authenticator can be used by an IPSEC gateway for verifying the identity of said user and granting him access to a corporate network.

37. Smart-card according to one of the claims 27 to 36, wherein at least one authenticator can be used by a remote location in a corporate network for verifying the identity of said user and granting him access to a remote domain.

20 38. Smart-card according to one of the claims 27 to 37, further comprising:

a synchronization private key for decrypting an old and a new secret encrypted with a corresponding synchronization public key,

comparison means for comparing said old decrypted secret

25 with the secret stored in said mobile equipment, and comparing said decrypted new secret with a new secret entered in said mobile equipment, means for replacing said secret stored in said mobile

equipment with said decrypted new secret when both comparisons are positive.

39. Smart-card comprising:
a synchronization private key for decrypting an old and a new
5 secret encrypted with a corresponding synchronization public key,
comparison means for comparing said old decrypted secret
with the secret stored in said mobile equipment, and comparing said
decrypted new secret with a new secret entered in said mobile equipment,
means for replacing said secret stored in said mobile
10 equipment with said decrypted new secret when both comparisons are
positive.
40. Smart-card according to claim 39, which is a SIM card.
41. Smart-card according to claim 39, which is a WIM card.

1/16

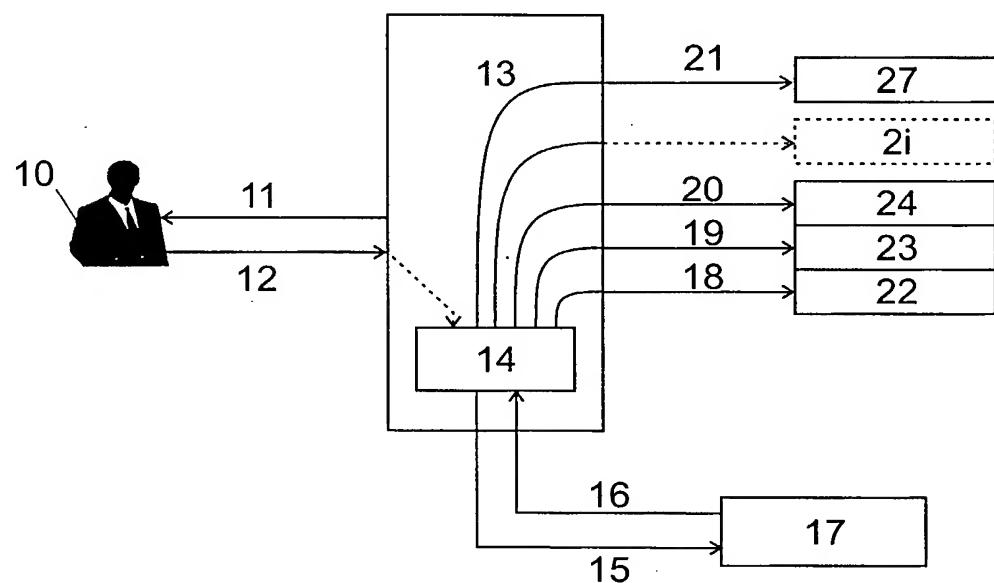


Fig.1

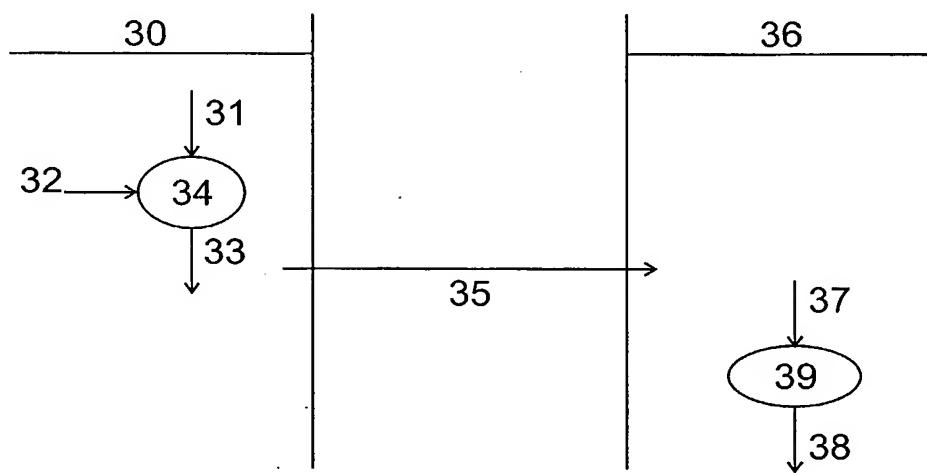


Fig.2

2/16

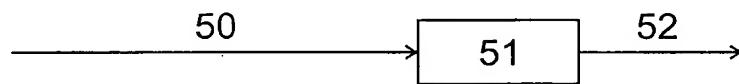


Fig.3

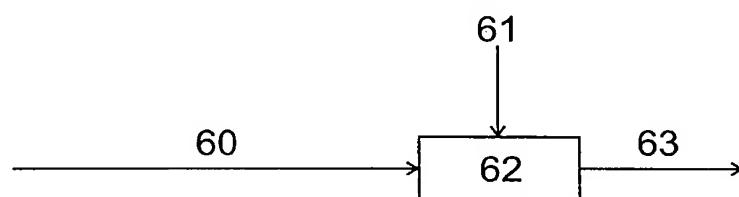


Fig.4

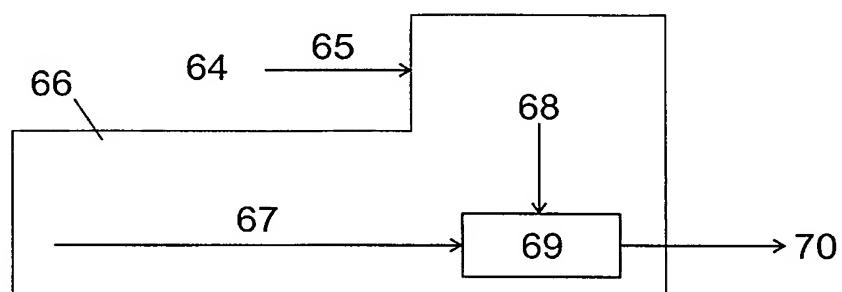


Fig.5

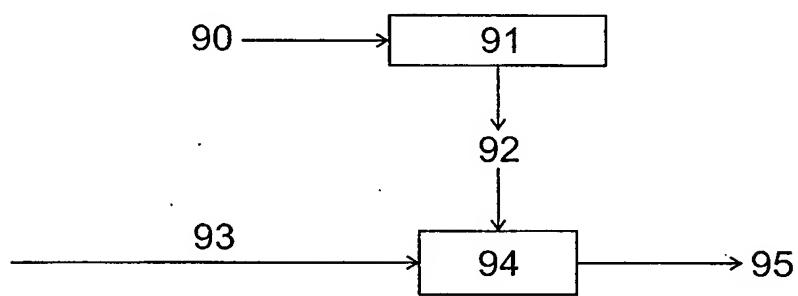


Fig.6

3/16

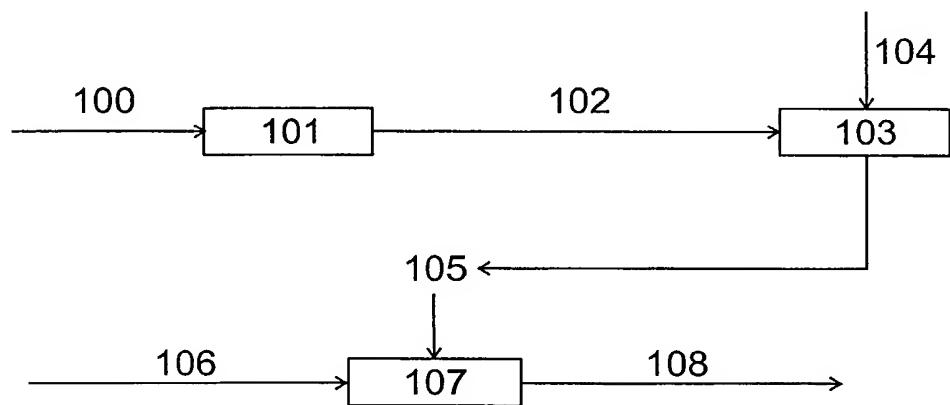


Fig. 7

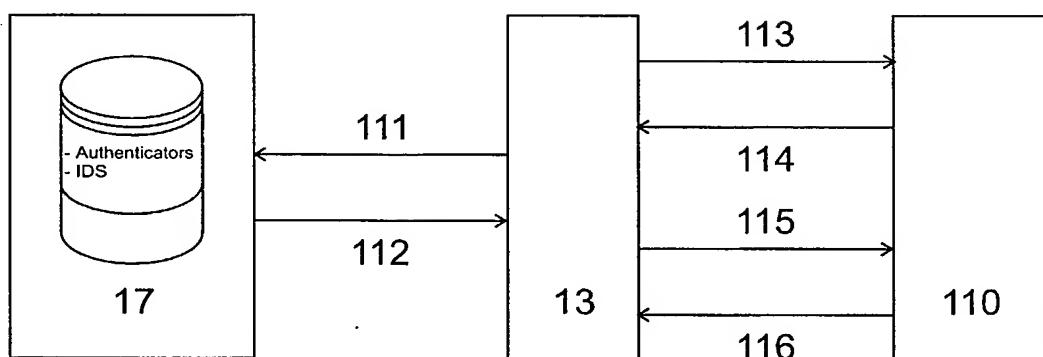


Fig. 8

4/16

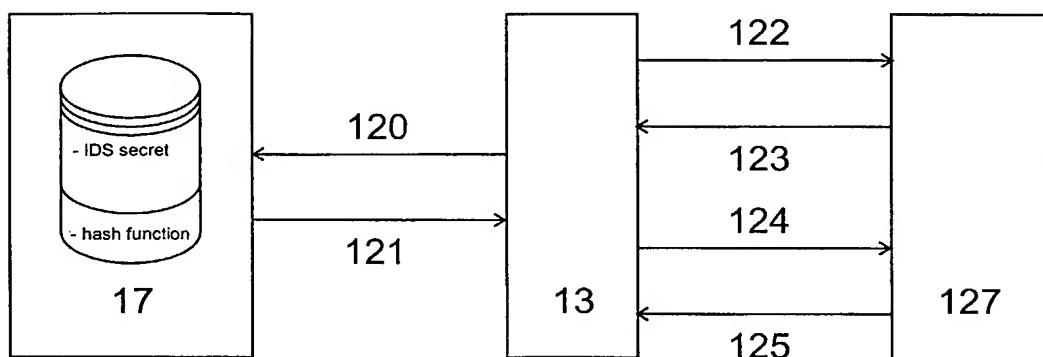


Fig. 9

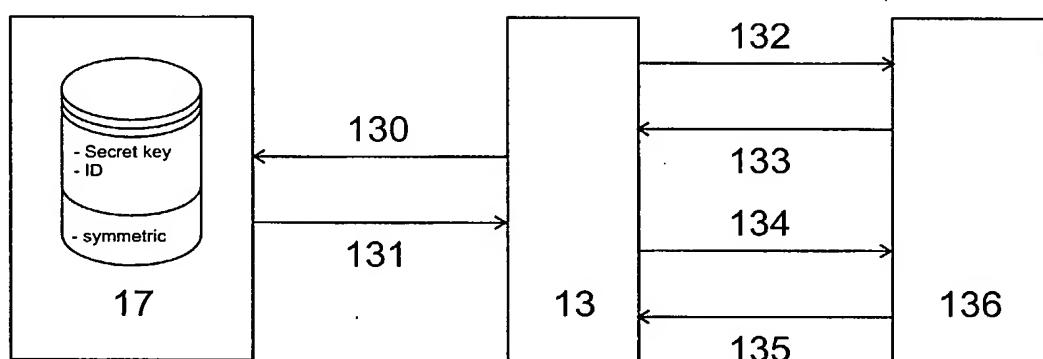


Fig. 10

5/16

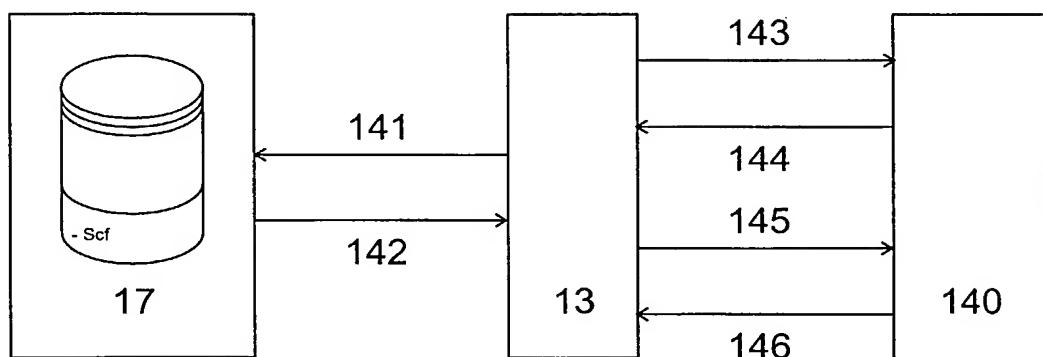


Fig.11

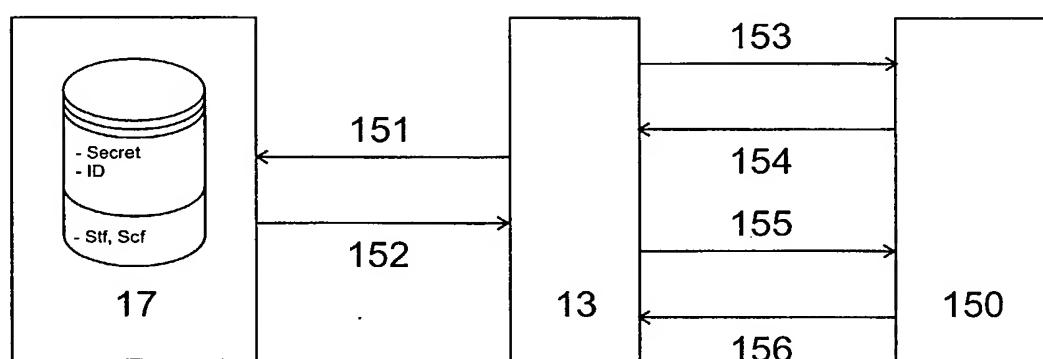


Fig. 12

6/16

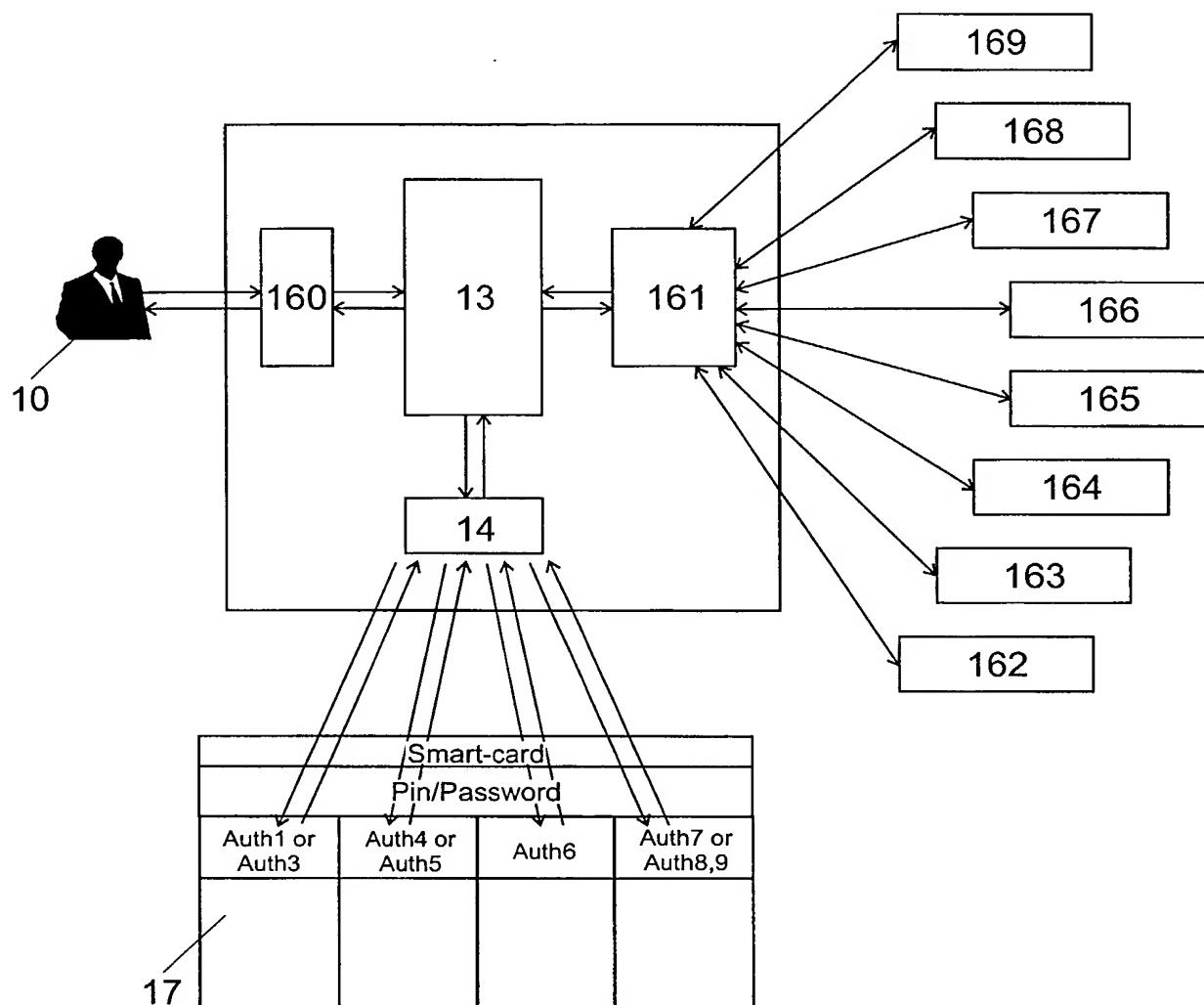


Fig. 13

7/16

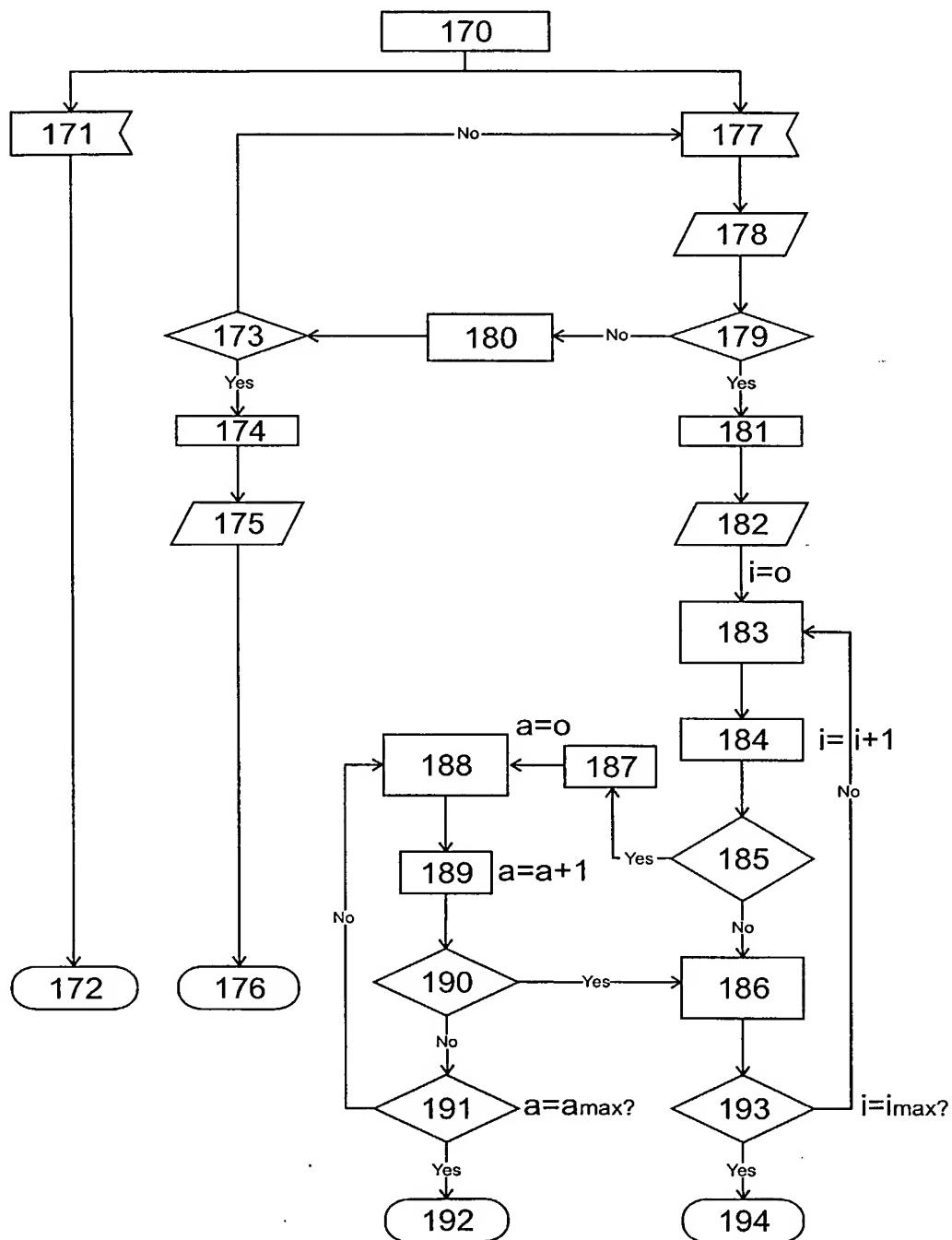


Fig. 14

8/16

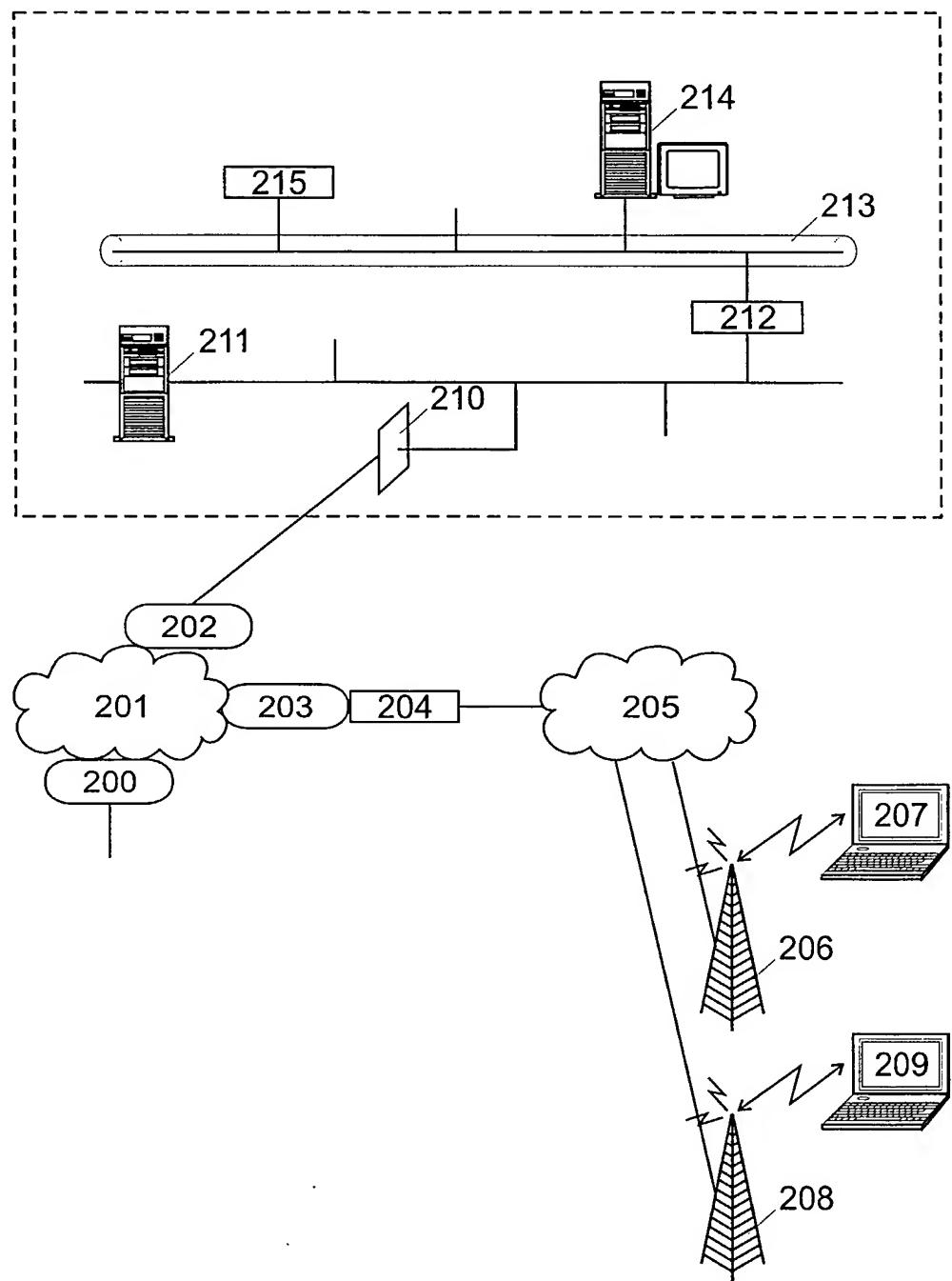


Fig. 15

9/16

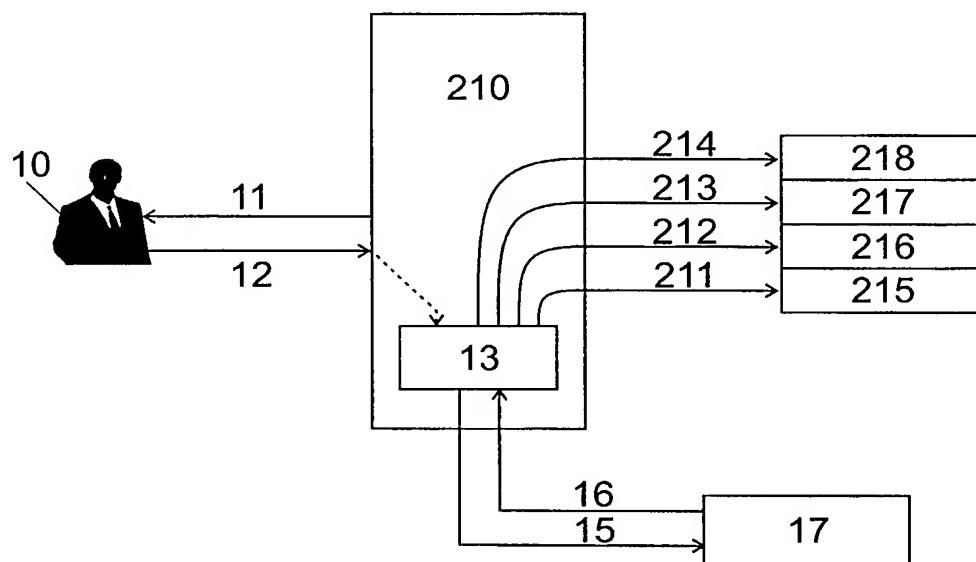


Fig.16

10/16

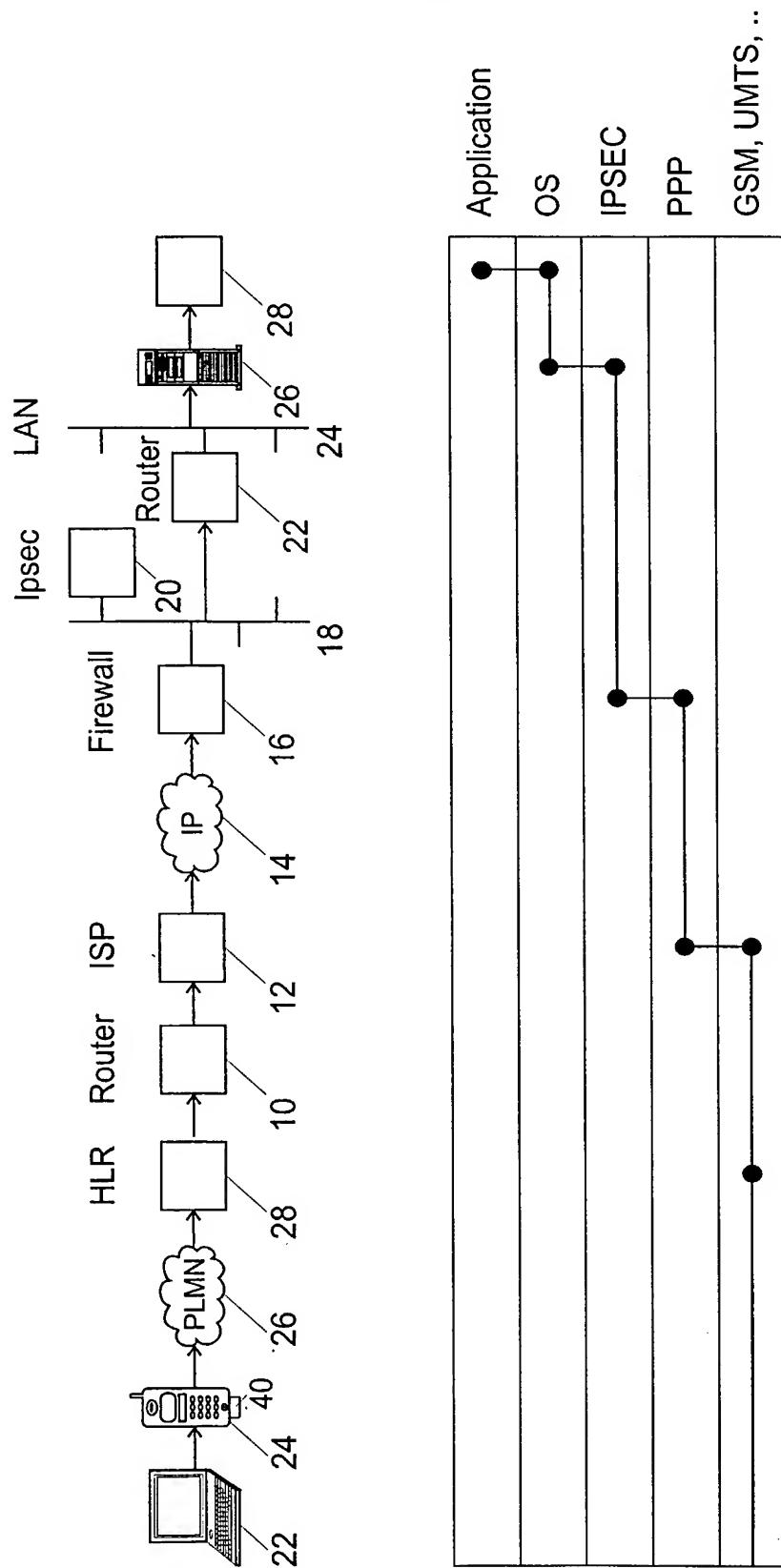


Fig. 16a

11/16

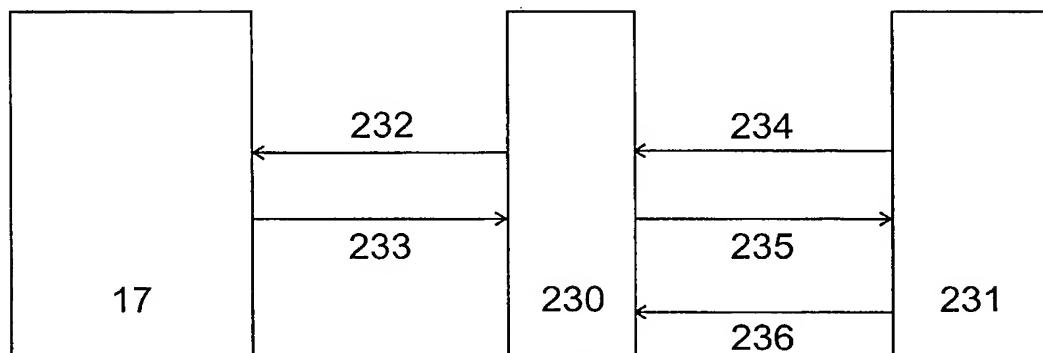


Fig. 17

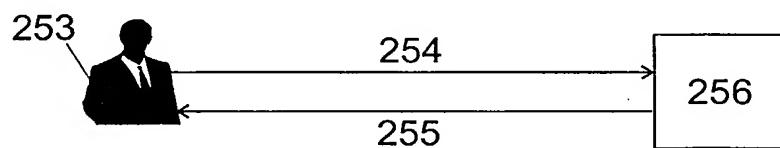


Fig. 18

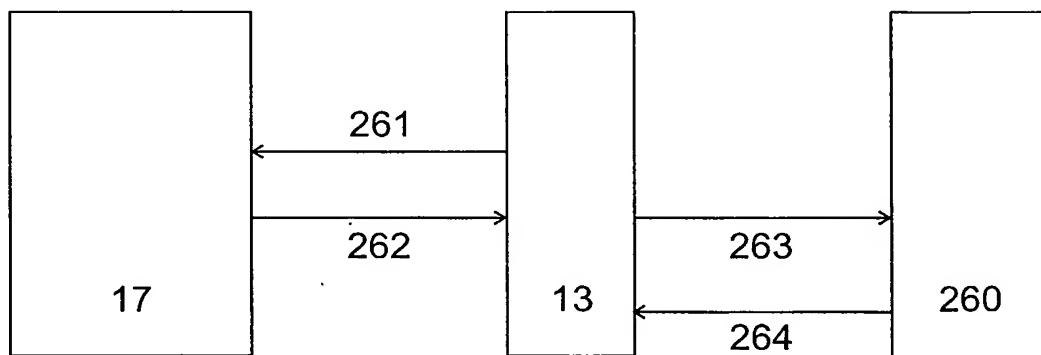


Fig. 19

12/16

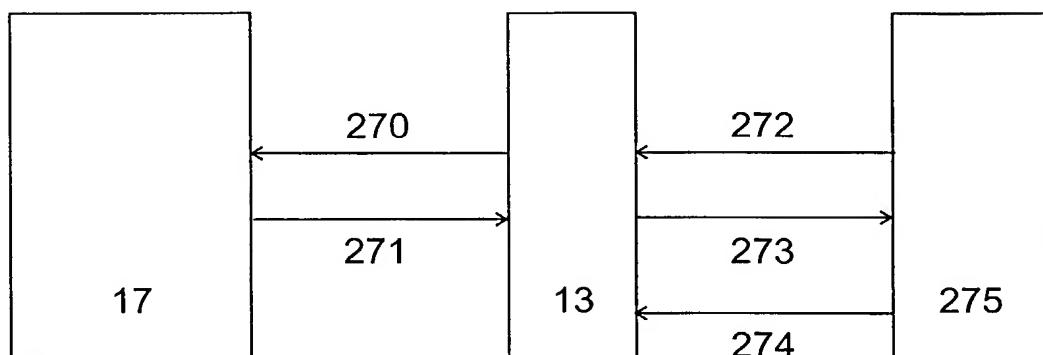


Fig. 20

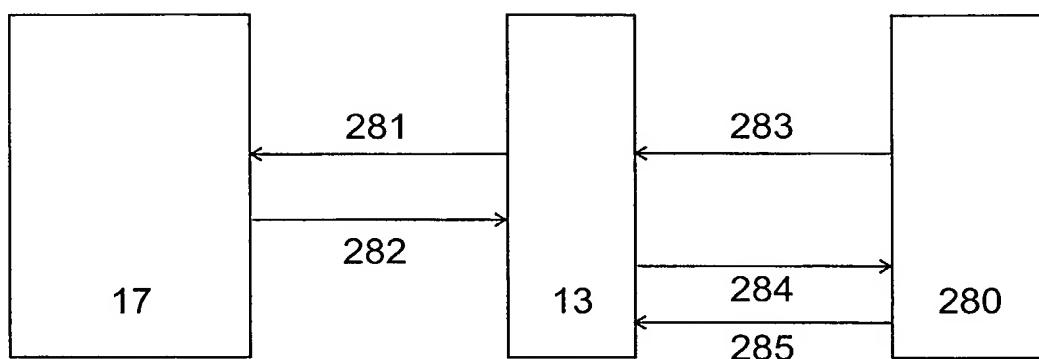


Fig. 21

13/16

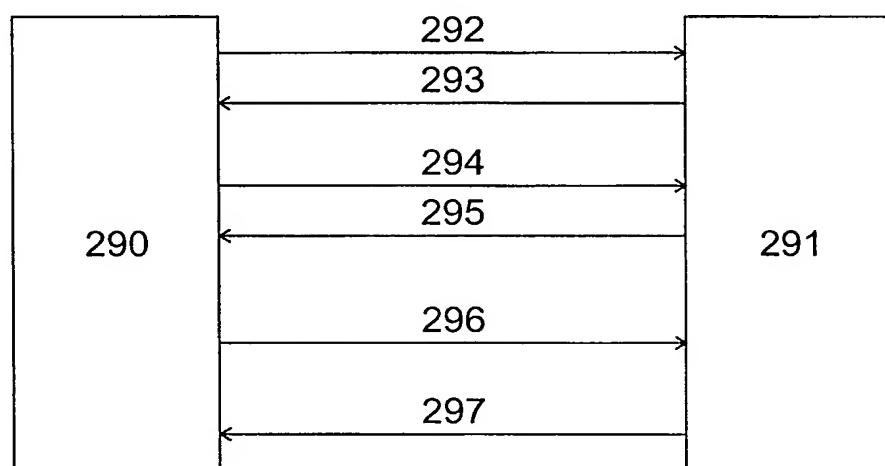


Fig. 22

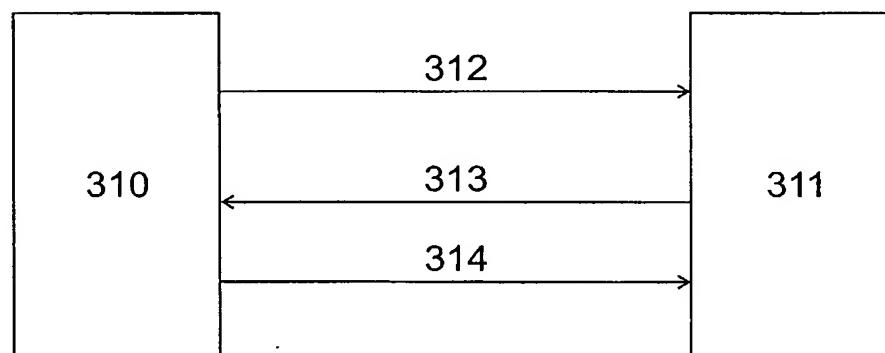


Fig. 23

14/16

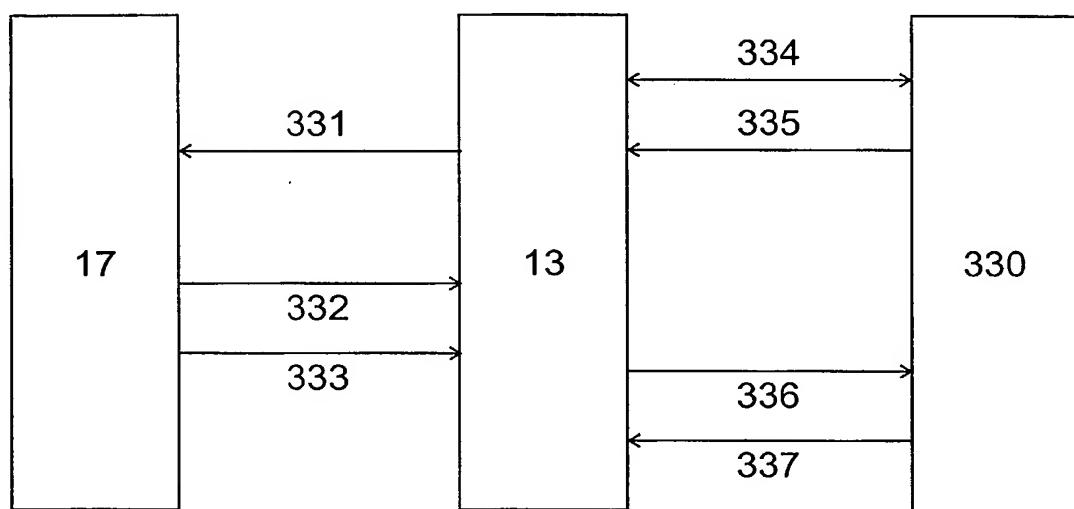


Fig. 24

15/16

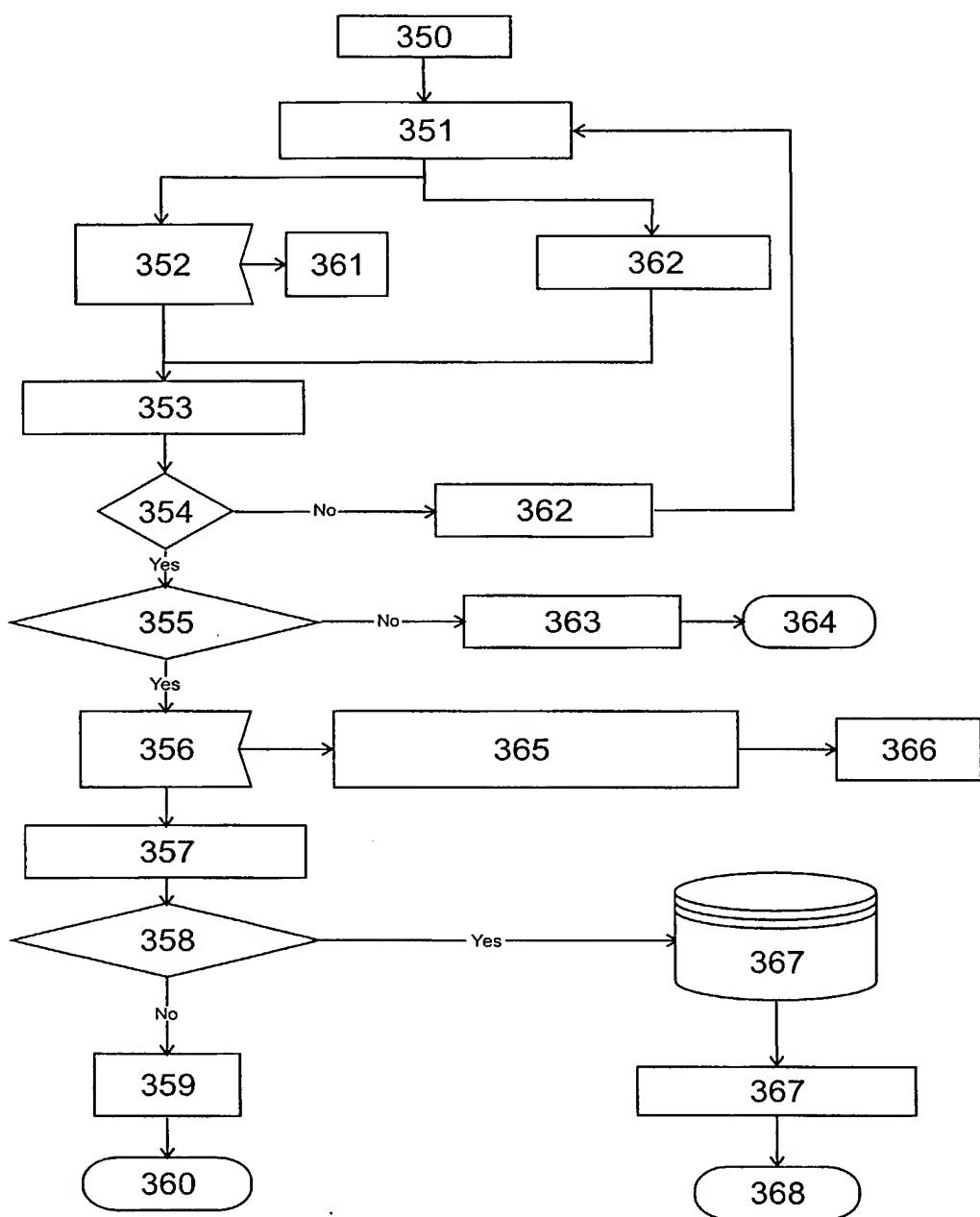


Fig. 25

16/16

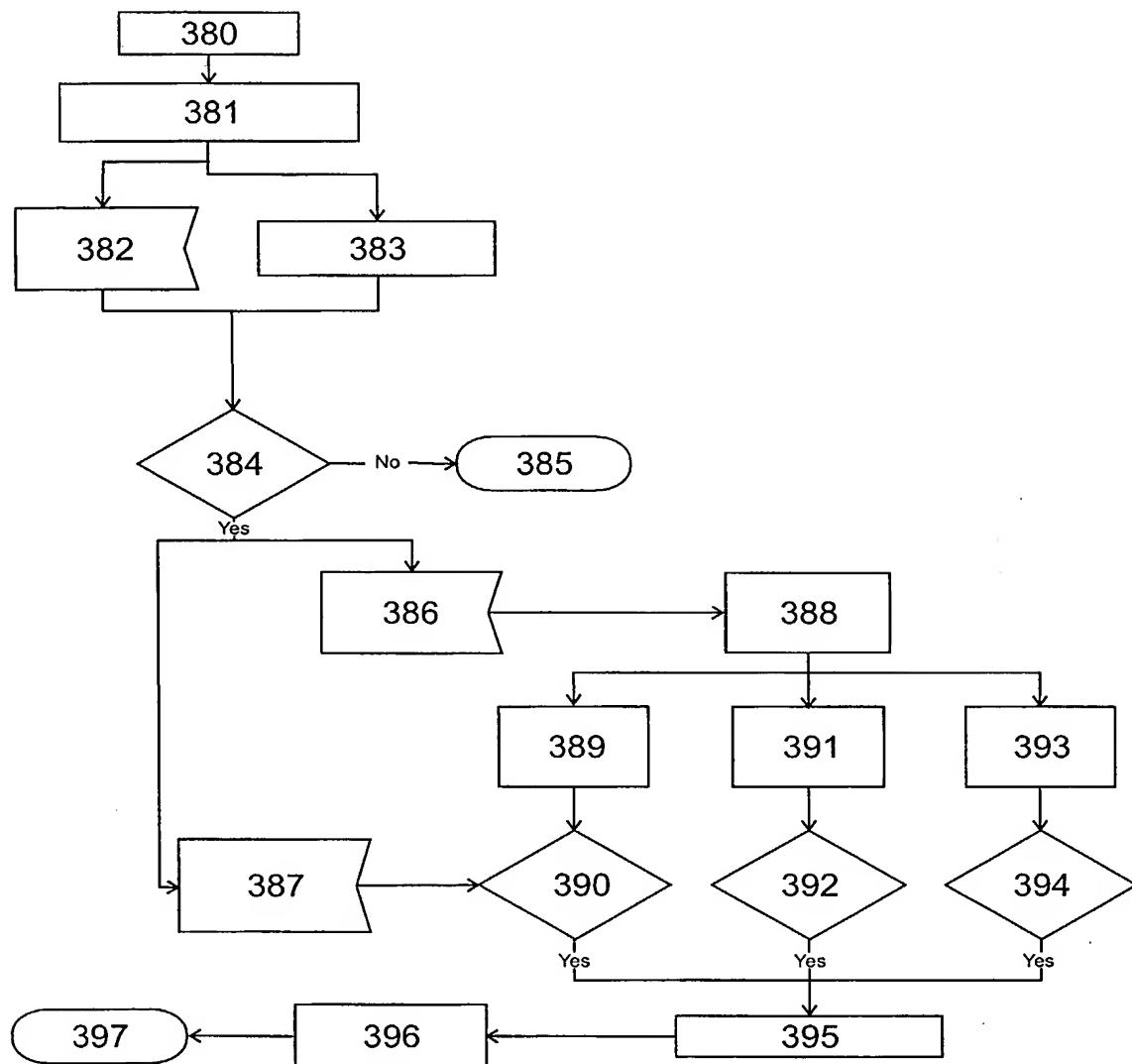


Fig. 26

INTERNATIONAL SEARCH REPORT

Int'l Application No
PCT/CH 00/00438A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 32301 A (ERICSSON TELEFON AB L M) 23 July 1998 (1998-07-23) page 5, line 14 -page 9, line 15; figure 1	1-20, 26-38
A	---	23,24, 40,41
A	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) column 2, line 23 - line 46 column 2, line 56 -column 3, line 38 column 5, line 5 - line 44 column 6, line 62 -column 7, line 61 column 10, line 18 - line 31 column 10, line 51 - line 60 column 13, line 4 - line 24 column 14, line 52 - line 65 column 17, line 12 - line 36 figure 2 ---	4,12,26, 27,32
		-/-

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

22 November 2000

13/12/2000

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

Int'l Application No
PCT/CH 00/00438

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES, VAN OORSCHOT, VANSTONE : "Handbook of Applied Cryptography" 1997 , CRC PRESS , BOCA RATON, FLORIDA 33431, USA XP002153614 ISBN: 0-8493-8523-7 page 506 -page 508 ---	21-25, 39-41
A		20, 38
A	INOUE A ET AL: "IP LAYER SECURITY AND MOBILITY SUPPORT DESIGN POLICY AND AN IMPLEMENTATION" GLOBAL NETWORK EVOLUTION: CONVERGENCE OR COLLISION? TORONTO, SEPT. 21 - 26, 1997, TORONTO, PINNACLE GROUP, CA, 21 September 1997 (1997-09-21), pages 571-577, XP000720565 page 571 -page 574 ---	17, 18, 35, 36
A	SCHULTZ E E: "Windows NT Security: Kudos, Concerns, And Prescriptions" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, NL, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 18, no. 3, 1999, pages 204-210, XP004164021 ISSN: 0167-4048 page 205 -page 206 -----	6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CH 00/00438

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9832301	A 23-07-1998	US 6061346 A		09-05-2000
		AU 725656 B		19-10-2000
		AU 5684698 A		07-08-1998
		BR 9806769 A		16-05-2000
		CN 1250578 T		12-04-2000
		EP 0953265 A		03-11-1999
US 5778071	A 07-07-1998	US 5546463 A		13-08-1996
		AU 4147097 A		06-03-1998
		EP 0916210 A		19-05-1999
		WO 9807255 A		19-02-1998
		US 5878142 A		02-03-1999